Divisibility of Kato's Euler system and its applications to Mazur and Tate's refined conjecture of BSD type

博　士　論　文

Divisibility of Kato's Euler system and its applications to Mazur and Tate's refined conjecture of BSD type

（加藤のオイラー系の可除性と
メイザー・テイトの BSD 型精密化予想への応用）

太 田　和 惟

平 成 2 7 年

Divisibility of Kato's Euler system and its applications to Mazur and Tate's refined conjecture of BSD type

A thesis presented

by

Kazuto Ota

to

The Mathematical Institute

for the degree of

Doctor of Science

Tohoku University

Sendai, Japan

September, 2015

Acknowledgements

I would like to express my sincere gratitude to my advisor, Professor Shinichi Kobayashi for his insightful advice and continuous encouragement. Seminars and discussion with him were always inspiring me during my study at Tohoku University. Without his guidance, this thesis would not have been completed.

I am grateful to Professor Nobuo Tsuzuki and Professor Takao Yamazaki for giving me helpful comments and advice on this thesis.

A part of this thesis consists of a work that was completed while I was visiting l'Institute de Mathématiques de Jussieu. I would like to express my appreciation to Professor Jan Nekovář for his hospitality. During the stay, I was supported by the Strategic Young Researcher Overseas Visits Program for Accelerating Brain Circulation by JSPS. I would like to thank Professor Shigeaki Koike for organizing the support for me with the program.

I am grateful to Professor Masato Kurihara for informing me of his work related to the Mazur-Tate refined conjecture. I am also grateful to Doctor Matteo Longo for discussion and his answers to my questions. I would like to thank Doctor Chan-Ho Kim for showing me his note of talks of Robert Pollack.

I am thankful to members of Number Theory Seminar at Tohoku University who formed fruitful study groups with me. I would also like to thank Doctor Kazuki Sato and Doctor Yuken Miyasaka for their friendships and a lot of discussion.

I was supported by Grant-in-Aid for JSPS Fellows 12J04338.

Finally, I would like to express my sincere thanks to my parents and sister for their warm encouragement and supports.

Contents

Chapter 1

Introduction

The aim of this thesis is to prove a part of the Mazur-Tate refined conjecture of BSD type in many cases. It asserts mysterious relations between zeta functions of elliptic curves over $\mathbb{Q}$ and arithmetic invariants in terms of *Mazur-Tate elements*. Our main result shows that the order of vanishing of Mazur-Tate elements is greater than or equal to the Mordell-Weil rank.

1.1 Background

In number theory, it is believed that zeta functions, or L-functions, mysteriously relate to arithmetic invariants. For an elliptic curve E over $\mathbb{Q}$, the Birch and Swinnerton-Dyer conjecture (BSD conjecture, for short) asserts that the order of vanishing of the Hasse-Weil L-function $L(E,s)$ at $s=1$ is equal to the Mordell-Weil rank:

Conjecture 1.1.1 (The weak BSD conjecture)**.**

$$\mathrm{ord}_{s=1}(L(E,s)) = \mathrm{rank}(E(\mathbb{Q})).$$

The *full* BSD conjecture further asserts an interpretation of the leading coefficient of $L(E,s)$ in terms of arithmetic invariants of E. Today, there are general conjectures due to Beilinson [1], Bloch [3], [4] and Bloch-Kato [5] for L-functions of general motives. These conjectures relate arithmetic invariants to complex analytic behavior of L-functions of motives. On the other hand, the p-adic BSD conjecture, Iwasawa main conjecture and their generalization relate the p-adic aspects of arithmetic invariants to p-adic L-functions.

The Mazur-Tate refined conjecture of BSD type is a partial refinement of the p-adic BSD conjecture. To compare these two conjectures, we first review the weak p-adic BSD conjecture briefly. For simplicity, we assume that p is a good ordinary prime of E. Then,

the p-adic L-function $\mathscr{L}_{p,E}$ of E is an element of $\Lambda := \left(\varprojlim \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})]\right) \otimes \mathbb{Q}_p$ such that for every finite character χ of $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$, the evaluation $\chi(\mathscr{L}_{p,E})$ equals the algebraic part of the special value $L(E, \chi^{-1}, 1)$ up to an explicit factor. Let I be the augmentation ideal of Λ, that is, the ideal I is the kernel of the morphism $\Lambda \to \mathbb{Q}_p$ sending every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ to 1. We put $r_E = \mathrm{rank}(E(\mathbb{Q}))$. The weak p-adic BSD conjecture asserts that the order of vanishing of $\mathscr{L}_{p,E}$ is equal to r_E :

Conjecture 1.1.2 (The weak p-adic BSD conjecture)**.**

$$\mathscr{L}_{p,E} \in I^{r_E} \setminus I^{r_E+1}.$$

In [28], not only for powers of p but also for every positive integer S, Mazur-Tate constructed an element in $\mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\mu_S)/\mathbb{Q})]$ whose evaluations are also special values $L(E, \chi^{-1}, 1)$, and they proposed a conjecture connecting the elements with arithmetic invariants. We call the conjecture the *Mazur-Tate refined conjecture of BSD type*.

1.2 The Mazur-Tate refined conjecture of BSD type

The Mazur-Tate refined conjecture of BSD type consists of two parts. One is a conjecture on the order of vanishing of Mazur-Tate elements, and the other is a conjecture on the formula of leading coefficients of the elements. In this section, we review the former part. The other part is reviewed in Chapter 3.

For each positive integer S, we put $G_S = \mathrm{Gal}(\mathbb{Q}(\mu_S)/\mathbb{Q})$. The *Mazur-Tate element* θ_S constructed in [28] is an element of $\mathbb{Q}[G_S]$ such that for every character χ of G_S, the evaluation $\chi(\theta_S)$ equals the algebraic part of $L(E, \chi^{-1}, 1)$ up to an explicit factor. It is important that the denominators of θ_S are bounded as S varies, which implies the existence of non-trivial congruences between these special values as χ varies. One can construct the p-adic L-function as a certain limit of $\{\theta_{p^n}\}_n$, and then Mazur-Tate elements may be regarded as a refinement of the p-adic L-function.

We fix a positive integer S and a subring R of $\mathbb{Q}$ such that $\theta_S \in R[G_S]$. It is known that if E is a strong Weil curve, then $\theta_S \in \mathbb{Z}[1/tc(E)][G_S]$ for all $S > 0$, where $t := |E(\mathbb{Q})_{\mathrm{tors}}|$, and $c(E) \in \mathbb{Z}$ denotes the Manin constant, which is conjectured to be 1 in this case. We denote by I_S the augmentation ideal of $R[G_S]$, that is, the ideal I_S is the kernel of the map from $R[G_S]$ to R sending every $\sigma \in G_S$ to 1. The aim of this thesis is to prove the following conjecture in many cases.

Conjecture 1.2.1 (Mazur-Tate)**.** We denote by $\mathrm{sp}(S)$ the number of split multiplicative primes of E dividing S. Then, we have

$$\theta_S \in I_S^{r_E+\mathrm{sp}(S)}.$$

Remark 1.2.2. Unlike Conjecture 1.1.2, it may happen that $\theta_S \in I_S^{r_E+\mathrm{sp}(S)+1}$. We give some cases where it happens.

1. It is known that if $|G_S| \in R^\times$ then $I_S = I_S^2 = I_S^3 = \cdots$. Hence, if $\theta_S \in I_S$, then $\theta_S \in I_S^a$ for all $a \geq 1$.

2. We assume that $r_E = 0$, and let ℓ be a good prime such that the Hasse invariant a_ℓ is equal to 2. Although $r_E = 0$ and $\mathrm{sp}(\ell) = 0$, the norm relation of Mazur-Tate elements shows that $\theta_\ell \in I_\ell$ for any subring R of $\mathbb{Q}$ such that $\theta_S \in R[G_S]$. For example, if E is defined by $y^2 + y = x^3 - x^2 - 2x + 1$, then $\mathrm{rank}(E(\mathbb{Q})) = 0$, and the good primes $\ell \leq 100000$ satisfying $a_\ell = 2$ are $\ell =$ 2, 3, 5, 251, 983, 1009, 1051, 1669, 8219, 9397, 10477, 11789, 14461, 21773, 24019, 32117, 51239, 57737, 93199, 95747, 97859, 98711. The calculation is due to Sage [41].

We mention known results on this conjecture. It seems that there have been only a few results up to present. Tan [43] proved Conjecture 1.2.1 in many cases. However, he was assuming the validity of the full BSD conjecture not only over $\mathbb{Q}$ but also over cyclic extensions K of $\mathbb{Q}$ inside $\mathbb{Q}(\mu_S)$. In [22], for each good ordinary prime p with mild assumptions, Kurihara proved that $\theta_S \in \mathbb{Z}_{(p)} \otimes_R I_S^{r_E}$. However he was assuming the validity of the $\mu = 0$ conjecture on the structure of a Selmer group (cf. Remark [22, Remark 2] and [28, Proposition 3]). In order to use his result to obtain $\theta_S \in I_S^{r_E}$, we need to assume the $\mu = 0$ conjecture for all primes p not invertible in R. In their unpublished work, Emerton, Pollack and Weston seem to have proved Conjecture 1.2.1 at least when S is a power of a supersingular prime p.

Today, there are some analogues of the refined BSD conjecture in which certain elements play roles of Mazur-Tate elements. In [8], Darmon considered elements in $E(K_S) \otimes \mathbb{Z}[\mathrm{Gal}(K_S/K)]$ constructed from Heegner points, and proposed a similar conjecture to the Mazur-Tate conjecture. Here, K_S is the ring class field of an imaginary quadratic field K of conductor S. Moreover, he proved a part of his conjecture on the order of vanishing of his element. In [24], Longo-Vigni announced a generalization of Darmon's result for the case of Heegner cycles. Instead of the BSD conjecture for elliptic curves, Gross [15] and Darmon [10] formulated the *refined class number formulas* for number fields.

1.3 The main result

1.3.1 The statement

We suppose that E is an elliptic curve over $\mathbb{Q}$ of conductor N without complex multiplication. Let R be a subring of $\mathbb{Q}$ in which the primes p satisfying one of the following

conditions are invertible:

(i) p divides $6N \cdot |E(\mathbb{F}_p)| \prod_{\ell|N} [E(\mathbb{Q}_\ell) : E_0(\mathbb{Q}_\ell)]$, where for a prime ℓ, we denote by $E_0(\mathbb{Q}_\ell)$ the group of points in $E(\mathbb{Q}_\ell)$ whose reduction is a non-singular point of $E(\mathbb{F}_\ell)$,

(ii) The Galois representation of $G_{\mathbb{Q}}$ attached to the p-adic Tate module $T_p(E)$ is *not* surjective,

(iii) $p < r_E$.

By Serre [37], there are only finitely many primes satisfying (ii). Following Mazur [26], we call a good prime p an *anomalous prime* of E if p divides $|E(\mathbb{F}_p)|$. We note that if $E(\mathbb{Q})$ has a non-trivial torsion point, then there are at most three anomalous primes of E ([26, Lemma 8.18]). In particular, in this case, each prime $p \geq 5$ dividing $|E(\mathbb{F}_p)|$ satisfies (ii) (cf. [26, p. 249]). In this thesis, primes p *not* satisfying the conditions (i), (ii) or (iii) are of interest to us.

The main result of this thesis is the following.

Theorem 1.3.1 (Theorem 5.4.1)**.** *Let S be a square-free product of good primes ℓ with the following condition: if $\ell \equiv 1 \mod p$ for a prime p not invertible in R, then $E(\mathbb{F}_\ell)[p]$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or 0 (cf. (2.1.1)). Then, Conjecture* 1.2.1 *holds, that is,*

$$\theta_S \in I_S^{r_E}.$$

Remark 1.3.2.

1. For a good supersingular prime ℓ of E and a prime $p \geq 3$, if $\ell \equiv 1 \mod p$, then $E(\mathbb{F}_\ell)[p] = 0$. Thus, there are infinitely many S satisfying the assumption of Theorem 1.3.1.

2. We denote by $\pi_E(x)$ the number of primes ℓ such that $E(\mathbb{F}_\ell)$ is cyclic and $\ell \leq x$. Then, by [16, Theorem 1], if $E(\mathbb{Q})[2] \ncong \mathbb{Z}/2\mathbb{Z}^{\oplus 2}$, then we have $\pi_E(x) \gg x/\log^2(x)$.

3. According to [42, §3], by the condition (ii) above, we have $\theta_S \in R[G_S]$.

As a special case of Theorem 1.3.1, by using [7, Theorem 2] and [37, Théorèm 4′], we have the following corollary.

Corollary 1.3.3. *We assume that $E(\mathbb{Q})$ has a non-trivial torsion point. We put*

$$d = \max\left\{ r_E,\ \frac{4\sqrt{6}}{3} N \prod_{\ell|N} \left(1 + \frac{1}{\ell}\right)^{\frac{1}{2}} + 1 \right\},$$

and take $R = \mathbb{Z}[p^{-1}; p < d]$. Then, for every square-free product S of good supersingular primes, we have

$$\theta_S \in I_S^{r_E}.$$

Example 1.3.4. If E is defined by $y^2+xy+y=x^3-22x-24$, then E does not have complex multiplication, and satisfies $E(\mathbb{Q})\cong\mathbb{Z}^{\oplus 2}\oplus\mathbb{Z}/2\mathbb{Z}$, $N=1918$ and $d=8232.59\ldots$. The good supersingular primes ℓ with $\ell\leq 100000$ are $\ell=$ 41, 283, 311, 353, 383, 439, 491, 811, 823, 1319, 1439, 2203, 3301, 3557, 4091, 4111, 5087, 5279, 6691, 9323, 9949, 10139, 10667, 12113, 13327, 15377, 16631, 20743, 20807, 23159, 23831, 30161, 31391, 32051, 32603, 32633, 32969, 33107, 33317, 35999, 38669, 50627, 50723, 69431, 70619, 84059, 86351, 89759, 91631, 96017, 97301, 98563. The calculation is due to Sage [41].

We also prove a partial evidence of the Mazur-Tate conjecture (cf. Conjecture 3.3.7) on the *leading coefficient* of θ_S, which is defined as the image $\widetilde{\theta}_S$ in $I_S^{r_E}/I_S^{r_E+1}$.

Theorem 1.3.5 (Theorem 5.4.2)**.** *Let p be a prime not invertible in R and S a square-free product of good primes ℓ such that $\ell\equiv 1 \mod p$ and $E(\mathbb{F}_\ell)[p]$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or 0. If $\widetilde{\theta}_S\not\equiv 0 \mod pI_S^{r_E}/I_S^{r_E+1}$, then we have*

$$Ш[p]=0 \quad \textit{and} \quad p\nmid J_S,$$

where Ш is the Tate-Shafarevich group of E over $\mathbb{Q}$, and J_S denotes the order of the cokernel of the map $E(\mathbb{Q})\to\left(\oplus_{\ell|S}E(\mathbb{F}_\ell)\right)\bigoplus\left(\oplus_{\ell|N}E(\mathbb{Q}_\ell)/E_0(\mathbb{Q}_\ell)\right)$.

1.3.2 An outline of the proof

We briefly explain how to prove Theorem 1.3.1. The case $r_E=1$ follows from a result of Kato and Kolyvagin (cf. [36, Theorem 3.5.4]). Then, we may assume that $r_E\geq 2$. By a group ring theoretic argument (Lemma 5.1.4), we are reduced to proving that

$$\theta_S\in\mathbb{Z}_p\otimes_R I_S^{r_E} \text{ for all primes } p \text{ not invertible in } R. \tag{1.3.1}$$

We take a prime p not invertible in R. For each positive integer S, we denote by $\mathbb{Q}(S)$ the maximal p-extension of $\mathbb{Q}$ inside $\mathbb{Q}(\mu_S)$. We put $\Gamma_S=\mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q})$, and denote by I_{Γ_S} the augmentation ideal of $\mathbb{Z}_p[\Gamma_S]$. Let $\mathrm{Sel}(\mathbb{Q},E[p^\infty])$ denotes the (discrete) Selmer group. We put $T=T_p(E)$ and $r_{p^\infty}=\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}(\mathbb{Q},E[p^\infty]))$. We recall that $r_{p^\infty}\geq r_E$. Let $\{\mathfrak{z}_{Sp^n}\}_{S,n}\in\prod_{S,n}H^1(\mathbb{Q}(Sp^n),T)$ denote Kato's Euler system.

Our proof of (1.3.1) consists of three steps:

Step1. For S as in Theorem 1.3.1, we prove that

$$\sum_{\gamma\in\Gamma_S}\mathfrak{z}_S^{\gamma^{-1}}\otimes\gamma\in H^1(\mathbb{Q}(S),T)\otimes I_{\Gamma_S}^{\min\{r_{p^\infty}-1,p\}}. \tag{1.3.2}$$

Step 2. We connect $\sum\mathfrak{z}_S^{\gamma^{-1}}\otimes\gamma$ with θ_S, and have

$$\theta_S\in\mathbb{Z}_p\otimes_R I_S^{\min\{r_{p^\infty}-1,p\}}.$$

Step 3. We apply the p-parity conjecture, and obtain

$$\theta_S \in \mathbb{Z}_p \otimes_R I_S^{\min\{r_{p^\infty},p\}}.$$

Then, we show (1.3.1), and hence Theorem 1.3.1.

We next explain more details of each step.

Step 1. Our strategy for (1.3.2) is to modify an argument of Darmon [8] for Kato's Euler system. In [8], Darmon showed a similar result to (1.3.2) for Heegner points. His idea was to consider a generalization of Kolyvagin derivative which we call *Darmon-Kolyvagin derivative*. As Darmon did, we show that some derivatives of Kato's Euler system are divisible by a power of p (Theorem 4.3.10), and obtain (1.3.2). We note that Kato's Euler system and the Euler system of Heegner points have different norm relations and local conditions at p. Then, it is not straightforward to apply Darmon's argument to Kato's Euler system. See also Remark 1.3.6.

Step 2. Modifying ideas of Kurihara [21], Kobayashi [19] and Otsuki [33], we construct an element $c_S \in \oplus_{\lambda|p} E(\mathbb{Q}(S)_\lambda)$ such that if we denote by $\theta_{S,p}$ the image of θ_S in $\mathbb{Z}_p[\Gamma_S]$ under the natural surjection $\mathbb{Z}_p[G_S] \to \mathbb{Z}_p[\Gamma_S]$, then

$$\theta_{S,p} = \sum_{\gamma\in\Gamma_S} (c_S, \mathfrak{z}_S^{\gamma^{-1}})\gamma \quad \text{in } \mathbb{Z}_p[\Gamma_S].$$

Here, for a prime $\lambda|p$ of $\mathbb{Q}(S)$, we denote by $\mathbb{Q}(S)_\lambda$ the completion at λ and by $(-,-)$ the paring $\bigoplus_{\lambda|p} H^1(\mathbb{Q}(S)_\lambda, T) \times \bigoplus_{\lambda|p} H^1(\mathbb{Q}(S)_\lambda, T) \to \mathbb{Z}_p$ induced by the cup product (we regard the element c_S as an element of the cohomology by the Kummer map). Then by (1.3.2), we obtain $\theta_{S,p} \in I_{\Gamma_S}^{\min\{r_{p^\infty}-1,p\}}$. Since $p \nmid [G_S : \Gamma_S]$, by a group ring theoretic argument (Lemma 5.1.2), we have $\theta_S \in \mathbb{Z}_p \otimes I_S^{\min\{r_{p^\infty}-1,p\}}$.

Step 3. The p-parity conjecture, which is a theorem ([12, Theorem 1.4]) now, asserts that

$$r_{p^\infty} \equiv \mathrm{ord}_{s=1}(L(E,s)) \mod 2.$$

On the other hand, Mazur-Tate showed the sign of the "functional equation of θ_S" is the same as that of $L(E,s)$ (see Section 5.3). More specifically, it is shown that if $\theta_S \in \mathbb{Z}_p \otimes I_S^a \setminus I_S^{a+1}$ for some $a \geq 1$, then $a \equiv \mathrm{ord}_{s=1}(L(E,s)) \mod 2$. If we take $a = r_{p^\infty} - 1$ and we assume that $p \geq r_{p^\infty}$ and $\theta_S \notin I_S^{r_{p^\infty}}$, then we have a contradiction, and hence $\theta_S \in \mathbb{Z}_p \otimes_R I_S^{\min\{r_{p^\infty},p\}}$.

Remark 1.3.6. Instead of (1.3.2) one might expect that the element $\sum \mathfrak{z}_S^{\gamma^{-1}} \otimes \gamma$ belongs to $H^1(\mathbb{Q}(S), T) \otimes I_{\Gamma_S}^{\min\{r_{p^\infty},p\}}$ and conclude (1.3.1) with Step 2. However, unfortunately, our modification of Darmon's argument enables us to obtain only (1.3.2). The obstruction is due to the local condition of Kato's Euler system. In Darmon's case, each Heegner point is obviously a local rational point of E under the localization at p, and then he was able

to relate Heegner points to Selmer groups with the usual local condition at p. On the other hand, the element $\mathfrak{z}_S$ does not necessarily come from a local rational point under the localization map at p, and we can relate Kato's Euler system only to the strict Selmer group $H^1_{f,p}(\mathbb{Q}, E[p^\infty])$, whose localization at p is trivial (cf. Remarks 4.3.12). We note that the pairing $(-,-)$ in Step 2 is trivial on $\bigoplus_{\lambda|p} E(\mathbb{Q}(S)_\lambda) \times \bigoplus_{\lambda|p} E(\mathbb{Q}(S)_\lambda)$, and hence if the element $\mathfrak{z}_S$ comes from a rational point under the localization at p, then the Mazur-Tate element θ_S is identically equal to zero. Hence, we cannot generally expect that $\mathfrak{z}_S$ comes from a rational point under the localization. Then, since the $\mathbb{Z}_p$-corank of the strict Selmer group is not necessarily greater than $r_{p^\infty} - 1$, we obtain only (1.3.2), and we need an additional argument to conclude Theorem 1.3.1. Our idea is to use the p-parity conjecture in Step 3.

A similar phenomenon also occurred in the proof of Kato's significant result ([18, Theorem 18.4]) which shows that $\mathscr{L}_{p,E} \in I^{r_E}$. A standard result on Euler systems by [17], [35] and [36] connects $\{\mathfrak{z}_{p^n}\}$ only with the strict Selmer group $H^1_{f,p}(\mathbb{Q}(p^\infty), E[p^\infty])$.

1.4 A result on a construction of rational points

We also give a result on a construction of rational points of E from some indivisibility of Euler systems. We show that if a certain derivative of an Euler system is not divisible by p, then it comes from a $\mathbb{Q}$-rational point of E.

Let $\{\mathfrak{z}_{Sp^n}\}_{S,n} \in \prod_{S,n} H^1(\mathbb{Q}(Sp^n), T)$ be Kato's Euler system. If $L(E,1) = 0$ and the Tate-Shafarevich group is finite, then $\mathfrak{z}_1 \in E(\mathbb{Q}) \otimes \mathbb{Q}_p \subseteq H^1(\mathbb{Q}, V_p(E))$. However, a relation between Euler systems and Selmer groups (cf. [36, Theorem 2.2.3]) shows that $\mathfrak{z}_1 = 0$ if $r_E \geq 2$. By taking derivatives of Euler systems, we have $\mathbb{Q}$-rational points (modulo p) even for greater r_E (notation is explained in Chapter 4):

Theorem 1.4.1 (Theorem 4.5.2)**.** *Let p be a prime not invertible in R. Let S be a square-free product of good primes ℓ such that $\ell \equiv 1 \mod p$ and $E(\mathbb{F}_\ell)[p]$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or 0. We assume that the natural map $E(\mathbb{Q})/p \to E(\mathbb{Q}_p)/p$ is surjective. Let D be a Darmon-Kolyvagin derivative with support S such that $\mathrm{ord}(D) = r_E - 1$. If $Dz_S \not\equiv 0 \mod pH^1(\mathbb{Q}(S), T)$, then $Ш[p] = 0$, and there exists a unique rational point $\kappa \in E(\mathbb{Q})/p \subseteq H^1(\mathbb{Q}, E[p])$ such that the restriction of κ to $H^1(\mathbb{Q}(S), E[p])$ coincides with the image of $D\mathfrak{z}_S$ in $H^1(\mathbb{Q}(S), E[p])$.*

Remark 1.4.2.

1. By Theorem 4.3.10, which is a key to (1.3.2), if $\mathrm{ord}(D) < r_E - 1$ then we have $D\mathfrak{z}_S \equiv 0 \mod pH^1(\mathbb{Q}(S), T)$.
2. For Heegner points, a similar result was obtained in [8, Proposition 5.10], where K-rational points are considered for imaginary quadratic fields K.

3. It seems difficult to check the assumption $D_{\mathfrak{z}_S} \not\equiv 0 \mod pH^1(\mathbb{Q}(S), T)$. We note that there is a conjecture by Perrin-Riou [34] as follows. When $L(E,1) = 0$, she conjectures that $\mathfrak{z}_1 \neq 0$ in $H^1(\mathbb{Q}, T)$ if and only if $L'(E,1) \neq 0$.

4. Zhang [46] recently proved a result on indivisibility of Kolyvagin derivatives of Heegner points.

1.5 Organization

This thesis is organized as follows.

In Chapter 2, we recall basic notion and results on elliptic curves. We also review the BSD conjecture.

In Chapter 3, we introduce Mazur-Tate elements, and state the Mazur-Tate refined conjecture of BSD type precisely.

In Chapter 4, we study divisibility of derivatives of Euler systems. The aim of this chapter is to show that some Darmon-Kolyvagin derivatives of Euler systems are divisible by a power of p (Theorem 4.3.10). Then, Step 1 of Subsection 1.3.2 is essentially completed in Section 4.3. In section 4.4, we show that a certain indivisibility of localization of Euler systems at p implies indivisibility of the Tate-Shafarevich group (Corollary 4.4.3). In section 4.5, we prove Theorem 1.4.1.

In Chapter 5, we prove our main result. In Section 5.2, we construct elements c_S as in Step 2 of Subsection 1.3.2, and relate Kato's Euler system with Mazur-Tate elements. We complete Step 3 in Section 5.3. Finally, we prove our main result in Section 5.4.

1.6 Notation

For a set X, we denote by $|X|$ the cardinality of X.

For an abelian group M and an integer n, we denote by $M[n]$ the group of the n-torsion points of M and by M_{tors} the maximal torsion subgroup of M. We also put $M/n = M/nM$.

For a field K, we denote by G_K the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$, where $\overline{K}$ is a separable closure of K. For a continuous G_K-module T, we denote by $H^*(K,T)$ the Galois cohomology $H^*(G_K, T)$. For a Galois extension L/K and a continuous $\mathrm{Gal}(L/K)$-module T, we put $H^*(L/K, T) = H^*(\mathrm{Gal}(L/K), T)$

We fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and put $\zeta_n = \exp(2\pi i/n)$ for $n \geq 0$. We also fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ for every prime p.

Chapter 2

Preliminaries on elliptic curves

In this chapter, we recall basic notion on elliptic curves, and state the BSD conjecture over $\mathbb{Q}$. Section 2.1 is devoted to fixing notation on elliptic curves. In Section 2.2, we review the statement of the BSD conjecture. We also recall the p-parity conjecture, which is used to prove our main result (cf. Subsection 1.3.2).

2.1 Elliptic curves

2.1.1 Generalities on elliptic curves

Let E be an elliptic curve over a perfect field K, that is, there exist $a_1, a_2, a_3, a_4, a_6 \in K$ such that E is isomorphic to the smooth subvariety of $\mathbb{P}^2_K$ as the Zariski closure of the affine variety defined by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

It is known that E is a commutative group variety whose origin is given by $[0 : 1 : 0]$. Then, for a field L containing K,

$$E(L) := \{[X : Y : Z] \in \mathbb{P}^2_K(L);\ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\}$$

is an abelian group.

The Kummer map For a positive integer n, we denote by $E[n]$ the group of n-torsion points in $E(\overline{K})$, which has a natural structure of discrete G_K-module. Then, we have an exact sequence of discrete G_K-modules

$$0 \to E[n] \to E(\overline{K}) \xrightarrow{n} E(\overline{K}) \to 0.$$

Taking Galois cohomology, we have an exact sequence

$$0 \to E(K)/n \to H^1(K, E[n]) \to H^1(K, E)[n] \to 0,$$

where $E(K)/n := E(K)/nE(K)$ and $H^1(K, E) := H^1(K, E(\overline{K}))$. We call the connecting map $E(K)/n \to H^1(K, E[n])$ the Kummer map. We often regard $E(K)/n$ as a subgroup of $H^1(K, E[n])$ by this map.

Torsion points For a prime p, we have the following.

1. If p is not equal to the characteristic $\mathrm{ch}(K)$ of K, then the group $E[p]$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$.
2. If $p = \mathrm{ch}(K)$, then the group $E[p]$ is trivial or isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

In particular, we have

$$E(K)[p] \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus j}, \quad \text{where } 0 \leq j \leq 2. \tag{2.1.1}$$

We note that $E(K)[p]$ is *cyclic* if $j = 0$ or 1.

In the case $p = \mathrm{ch}(K)$, we say E is *supersingular* if $E[p] = 0$, and say E is *ordinary* otherwise.

The Tate module For a prime p relatively prime to $\mathrm{ch}(K)$, we define the p-adic Tate module of E as

$$T_p(E) = \varprojlim_n E[p^n],$$

and put $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Then, we have a p-adic representation

$$G_K \to \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E)).$$

Since $T_p(E) \cong \mathbb{Z}_p^{\oplus 2}$, we have $G_K \to \mathrm{GL}_2(\mathbb{Z}_p)$.

2.1.2 Elliptic curves over local fields

Suppose that K is a discrete valuation field with perfect residue filed k. We denote by $\mathscr{O}_K$ the ring of integers and by $\mathfrak{m}$ the maximal ideal of $\mathscr{O}_K$.

Reduction We fix a *minimal* Weierstrass model of E over $\mathscr{O}_K$. Namely, we fix an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in \mathscr{O}_K)$$

which defines E over K, and whose discriminant is minimal (cf. [40, §VII.1]). By reducing this equation modulo $\mathfrak{m}$, we have a closed subvariety $\widetilde{E}$ of $\mathbb{P}^2_k$. We denote by $\widetilde{E}^{\mathrm{ns}}$ the set of nonsingular points of $\widetilde{E}$. Then, $\widetilde{E}^{\mathrm{ns}}$ satisfies one of the following:

(a) $\widetilde{E}^{\mathrm{ns}} = \widetilde{E}$, that is, the variety $\widetilde{E}$ is an elliptic curve over k.

(b) $\widetilde{E}^{\mathrm{ns}}(\overline{k}) \cong \overline{k}^{\times}$ as abelian groups.

(c) $\widetilde{E}^{\mathrm{ns}}(\overline{k}) \cong \overline{k}$ as abelian groups.

In the case (a), we say E has *good reduction*. In this case, we often write $E(k) = \widetilde{E}(k)$. In the case (b), we say E has *multiplicative reduction*. In this case, we say E has *split multiplicative reduction* if $\widetilde{E}^{\mathrm{ns}}(k) \cong k^{\times}$, and say E has *nonsplit multiplicative reduction* otherwise. In the case (c), we say E has *additive reduction*. When E does not have good reduction, we say E has bad reduction.

The reduction map For each element P of $E(K)$, there exist elements $X, Y, Z \in \mathscr{O}_K$ such that $P = [X : Y : Z]$ and at least one of X, Y, Z belongs to $\mathscr{O}_K^{\times}$. Then, by reducing $[X : Y : Z]$ modulo $\mathfrak{m}$, we obtain an element $\widetilde{P}$ of $\widetilde{E}(k)$, which is independent of the choice of X, Y, Z. By sending each $P \in E(K)$ to $\widetilde{P} \in \widetilde{E}(k)$, we have the *reduction map* $E(K) \to \widetilde{E}(k)$.

We define a subgroup $E_0(K) \subseteq E(K)$ as the inverse image of $\widetilde{E}^{\mathrm{ns}}(k)$ under the reduction map. By the existence of Néron model (cf. [23], [39]), it is known that $E(K)/E_0(K)$ is a finite abelian group (cf. [39, Chapter IV, Corollary 9.2]).

Local points In the following, we suppose that K is a finite extension of $\mathbb{Q}_\ell$ for a prime ℓ. Then, Hensel's lemma shows that the reduction map is surjective (cf. [40, Chapter VII, Proposition 2.1]). Thus, we have an exact sequence

$$0 \to \hat{E}(\mathscr{O}_K) \to E_0(K) \to \widetilde{E}^{\mathrm{ns}}(k) \to 0, \tag{2.1.2}$$

where $\hat{E}$ is the formal group of E over $\mathscr{O}_K$. We note that $E(K)/E_0(K)$ and $\widetilde{E}^{\mathrm{ns}}(k)$ are finite and $\hat{E}(\mathscr{O}_K)$ is isomorphic to a direct sum of $\mathbb{Z}_\ell^{[K:\mathbb{Q}_\ell]}$ and a finite group. Hence, the torsion group $E(K)_{\mathrm{tors}}$ is finite and

$$E(K) \cong \mathbb{Z}_\ell^{[K:\mathbb{Q}_\ell]} \oplus E(K)_{\mathrm{tors}}. \tag{2.1.3}$$

Proposition 2.1.1. *Let K be a finite extension of $\mathbb{Q}_\ell$ for a prime ℓ and E an elliptic curve over K with good reduction. We take a prime p not equal to ℓ. Then,*

$$E(K)/p \cong E(K)[p] \cong E(k)[p].$$

In particular,

$$E(K)/p \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus j}, \quad \text{where } 0 \leq j \leq 2.$$

Proof. By (2.1.3), we have

$$E(K)/p \cong E(K)_{\mathrm{tors}}/p. \tag{2.1.4}$$

Since $E(K)_{\mathrm{tors}}$ is finite, by the structure theorem for finite abelian groups, we have a non-canonical isomorphism

$$E(K)_{\mathrm{tors}}/p \cong E(K)[p]. \tag{2.1.5}$$

Since E has good reduction and $\ell \neq p$, Hensel's lemma shows that

$$E(K)[p] \cong E(k)[p].$$

Hence, by (2.1.4) and (2.1.5), we obtain

$$E(K)/p \cong E(k)[p].$$

□

Galois cohomology We denote by K^{ur} the maximal unramified extension of K, and put

$$\begin{aligned} H^1_{\mathrm{ur}}(K, T_p(E)) &= \ker(H^1(K, T_p(E)) \to H^1(K^{\mathrm{ur}}, T_p(E))), \\ H^1_{\mathrm{ur}}(K, E[m]) &= \ker(H^1(K, E[m]) \to H^1(K^{\mathrm{ur}}, E[m])) \ \text{ for } m \geq 0. \end{aligned}$$

We note that if E has good reduction then

$$H^1_{\mathrm{ur}}(K, E[m]) = H^1(K^{\mathrm{ur}}/K, E[q]) = H^1(\mathbb{F}_\ell, E[q]).$$

Proposition 2.1.2. *We assume that E has good reduction. Let p be a prime not equal to ℓ. For a power q of p, we have*

$$E(K)/q = H^1_{\mathrm{ur}}(K, E[q]),$$

where $E(K)/q$ is regarded as a subgroup of $H^1(K, E[q])$ by the Kummer map.

PROOF. First we show that $E(K)/q \subseteq H^1_{\mathrm{ur}}(K, E[q])$. We take an element x of $E(K)/q$. Since $\ell \neq p$, by (2.1.3) we have $E(K)/q \cong E(K)[p^\infty] \otimes \mathbb{Z}/q\mathbb{Z}$. We take $P \in E(K)[p^\infty]$ whose image in $E(K)/q$ is equal to x. Then, there exists an element $Q \in E(\overline{K})[p^\infty]$ such that $qQ = P$. Since E has good reduction and $\ell \neq p$, we have $Q \in E(K^{\mathrm{ur}})[p^\infty]$. By the definition of the Kummer map, if we regard x as a cocycle, then for $\sigma \in G_K$

$$x(\sigma) = (\sigma - 1)Q \in E[q].$$

Since $Q \in E(K^{\mathrm{ur}})$, the restriction of x to $H^1(K^{\mathrm{ur}}, E)$ is zero. Then, we show that $x \in H^1_{\mathrm{ur}}(K, E[q])$.

Conversely, we take an element $y \in H^1_{\mathrm{ur}}(K, E[q])$. Since E has good reduction,

$$H^1_{\mathrm{ur}}(K, E[q]) = H^1(K^{\mathrm{ur}}/K, E[q]).$$

Since $H^2(K^{\mathrm{ur}}/K, T_p(E)) = 0$, by taking Galois cohomology with respect to the exact sequence

$$0 \to T_p(E) \overset{\times q}{\to} T_p(E) \to E[q] \to 0,$$

we have an exact sequence

$$H^1(K^{\mathrm{ur}}/K, T_p(E)) \overset{\times q}{\to} H^1(K^{\mathrm{ur}}/K, T_p(E)) \to H^1(K^{\mathrm{ur}}/K, E[q]) \to 0.$$

Then, we have a lift $\widetilde{y} \in H^1(K^{\mathrm{ur}}/K, T_p(E))$ of y. We denote by Fr the generator of $\mathrm{Gal}(K^{\mathrm{ur}}/K)$. We note that

$$H^1(K^{\mathrm{ur}}/K, T_p(E)) \otimes \mathbb{Q}_p = (T_p(E)/(\mathrm{Fr} - 1)T_p(E)) \otimes \mathbb{Q}_p = V_p(E)/(\mathrm{Fr} - 1)V_p(E) = 0,$$

where the last equality follows from the fact that each eigenvalue of Fr on $V_p(E)$ is not 1. Thus,

$$H^1(K^{\mathrm{ur}}/K, T_p(E)) \subseteq H^1(K, T_p(E))_{\mathrm{tors}}. \tag{2.1.6}$$

By taking Galois cohomology with respect to the exact sequence

$$0 \to T_p(E) \to V_p(E) \to E[p^\infty] \to 0,$$

we have an exact sequence

$$0 \to E(K)[p^\infty] \to H^1(K, T_p(E)) \to H^1(K, V_p(E)),$$

which implies that $H^1(K, T_p(E))_{\mathrm{tors}} = E(K)[p^\infty]$. By (2.1.6), we obtain $\widetilde{y} \in E(K)[p^\infty]$, and hence $y \in E(K)/q$. □

Let $\mathscr{E}$ be the Néron model of E over $\mathrm{Spec}(\mathscr{O}_K)$. We denote by $\pi_0(\mathscr{E}_{\overline{k}})$ the group of connected components of $\mathscr{E}_{\overline{k}}$, which has a natural action of $G_k = G_K/I_K$. Here I_K denotes the inertia group. Then, we have a natural G_k-invariant isomorphism (cf. [39, Corollary 9.2 in Chapter IV])

$$E(K^{\mathrm{ur}})/E_0(K^{\mathrm{ur}}) \cong \pi_0(\mathscr{E}_{\overline{k}}).$$

Proposition 2.1.3. *We have*

$$H^1(G_K/I_K, E(K^{\mathrm{ur}})) \cong H^1(G_k, \pi_0(\mathscr{E}_{\overline{k}})).$$

Proof. This is [30, Proposition 3.8 in Chapter I]. □

Duality For $n \in \mathbb{Z}$ relatively prime to $\mathrm{ch}(K)$, we have the Weil paring, which is a perfect G_K-invariant paring

$$E[n] \times E[n] \to \mu_n,$$

where μ_n is the group of n-th roots of unity in $\overline{K}$. By using the Weil pairing and local Tate duality, we have a perfect pairing

$$H^1(K, E[n]) \times H^1(K, E[n]) \xrightarrow{\cup} H^2(K, \mu_n) \cong \mathbb{Z}/n\mathbb{Z},$$

where $\cup$ denotes the cup product, and the last isomorphism is the *invariant map*.

Theorem 2.1.4. *Under the cup product above, the subgroup $E(K)/n$ of $H^1(K, E[q])$ is the exact annihilator of itself. In other words, we have a perfect pairing*

$$E(K)/n \times H^1(K, E)[n] \to \mathbb{Z}/n\mathbb{Z}.$$

Proof. In [30], This is Corollary 3.4 of Chapter I. □

2.1.3 Elliptic curves over number fields

Let K be a finite extension of $\mathbb{Q}$. For an elliptic curve E over K, we call $E(K)$ the *Mordell-Weil group*. The Mordell-Weil theorem (cf. [40]) says:

Theorem 2.1.5. *The Mordell-Weil group $E(K)$ is finitely generated over $\mathbb{Z}$, that is, we have*

$$E(K) \cong \mathbb{Z}^{\oplus r} \oplus T$$

for some $r \geq 0$ and a finite abelian group T.

The Selmer group and the Tate-Shafarevich group For $n \geq 0$, we put

$$\mathrm{Sel}(K, E[n]) = \ker\left(H^1(K, E[n]) \to \prod_{\lambda:\text{places}} \frac{H^1(K_\lambda, E[n])}{E(K_\lambda)/n}\right),$$

where K_λ is the completion of K at λ. By taking the direct limit with respect to $E[n] \hookrightarrow E[m]$ for $n|m$, we define the Selmer group $\mathrm{Sel}(E/K)$ by

$$\mathrm{Sel}(E/K) = \varinjlim \mathrm{Sel}(K, E[n]).$$

In other words,

$$\mathrm{Sel}(E/K) := \ker\left(H^1(K, E_{\mathrm{tors}}) \to \prod_{\lambda:\text{places}} \frac{H^1(K_{\lambda:}, E_{\mathrm{tors}})}{E(K_\lambda) \otimes \mathbb{Q}/\mathbb{Z}}\right).$$

The Tate-Shafarevich group $Ш(E/K)$ is defined by

$$Ш(E/K) = \ker\left(H^1(K, E) \to \prod_{\lambda:\text{places}} H^1(K_\lambda, E)\right),$$

which is a torsion group and is conjectured to be finite:

Conjecture 2.1.6. The Tate-Shafarevich group $Ш(E/K)$ is finite.

By the exact sequences

$$0 \to E(K) \otimes \mathbb{Q}/\mathbb{Z} \to H^1(K, E_{\mathrm{tors}}) \to H^1(K, E) \to 0,$$
$$0 \to E(K_\lambda) \otimes \mathbb{Q}/\mathbb{Z} \to H^1(K_\lambda, E_{\mathrm{tors}}) \to H^1(K_\lambda, E) \to 0$$

for each λ, we have the exact sequence

$$0 \to E(K) \otimes \mathbb{Q}/\mathbb{Z} \to \mathrm{Sel}(E/K) \to Ш(E/K) \to 0.$$

For a prime p, we denote by $\mathrm{Sel}(K, E[p^\infty])$ the p-torsion part of $\mathrm{Sel}(E/K)$. Then, we have the following exact sequence

$$0 \to E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}(K, E[p^\infty]) \to Ш(E/K)[p^\infty] \to 0,$$

and have $\mathrm{rank}(E(K)) \leq \mathrm{rank}_{\mathbb{Z}_p}(\mathrm{Sel}(K, E[p^\infty])^\vee)$, where we denote by $\mathrm{Sel}(K, E[p^\infty])^\vee$ the Pontryagin dual $\mathrm{Hom}(\mathrm{Sel}(K, E[p^\infty]), \mathbb{Q}_p/\mathbb{Z}_p)$. We put

$$\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}(K, E[p^\infty])) = \mathrm{rank}_{\mathbb{Z}_p}(\mathrm{Sel}(K, E[p^\infty])^\vee).$$

2.2 The Birch and Swinnerton-Dyer conjecture

Suppose that E is an elliptic curve over $\mathbb{Q}$ of conductor N. We recall that N is a product of the primes in which E has bad reduction (see [39, Chapter IV, §11] for the precise definition of conductor).

We first define the Hasse-Weil L-function $L(E,s)$ of E, and review its property.

Definition 2.2.1. We define the Hasse-Weil L-function $L(E,s)$ of E by

$$L(E,s) = \prod_{\ell:\text{primes}} \left(1 - a_\ell(E)\ell^{-s} + \epsilon(\ell)\ell^{1-2s}\right)^{-1},$$

where for each prime ℓ, we put

$$a_\ell(E) = \begin{cases} \ell + 1 - |E(\mathbb{F}_\ell)| & \text{if } \ell \nmid N \\ 1 & \text{if } \ell \text{ is a split multiplicative prime} \\ -1 & \text{if } \ell \text{ is a nonsplit multiplicative prime} \\ 0 & \text{if } \ell \text{ is an additive prime,} \end{cases} \qquad \epsilon(\ell) = \begin{cases} 1 & \text{if } \ell \nmid N \\ 0 & \text{if } \ell | N. \end{cases}$$

By Hasse's theorem (cf. [40, Chapter V, Theorem 1.1]), the function $L(E,s)$ converges for all s with $\mathrm{Re}(s) > 3/2$. For a Dirichlet character χ modulo S, we also define

$$L(E,\chi,s) = \prod_{\ell \nmid S} \left(1 - a_\ell(E)\chi(\ell)\ell^{-s} + \epsilon(\ell)\chi(\ell)^2\ell^{1-2s}\right)^{-1}.$$

By the Shimura-Taniyama conjecture, which was proved by Wiles [45], Taylor-Wiles [44] and Breuil-Conrad-Diamond-Taylor [6], we have the following.

Theorem 2.2.2. *There exists a unique newform f of weight 2 for $\Gamma_0(N)$ with trivial character such that*

$$L(f,s) = L(E,s).$$

In particular, $L(E,s)$ has an analytic continuation to the whole complex s-plane, and has a functional equation relating its value at s to its value at $2-s$.

We fix a *global minimal Weierstrass model* of E over $\mathbb{Z}$. Namely, we fix an equation defining E over $\mathbb{Q}$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in \mathbb{Z})$$

which is a minimal Weierstrass model of E over $\mathbb{Z}_\ell$ for every prime ℓ. We put

$$\omega = \frac{dx}{2y + a_1x + a_3}.$$

Then, $H^0(E, \Omega^1_{E/\mathbb{Q}}) = \mathbb{Q}\omega$. We call ω the *Néron differential*. We define the real period $\Omega_E > 0$ by

$$\Omega_E = \int_{E(\mathbb{R})} |\omega|.$$

We denote by $\hat{h}$ the real-valued *canonical height* (cf. [40, VIII.9]) on $E/\mathbb{Q}$, and define the *canonical height pairing* $\langle -, - \rangle$ on $E(\mathbb{Q}) \times E(\mathbb{Q})$ as

$$\langle P, Q \rangle = \frac{1}{2}\left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right) \in \mathbb{R}.$$

We fix a $\mathbb{Z}$-basis $\{P_i\}$ of $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$, and define

$$\mathrm{Reg}(E/\mathbb{Q}) = \det(\langle P_i, P_j \rangle) \in \mathbb{R}.$$

For each prime $\ell | N$, we put

$$m_\ell = [E(\mathbb{Q}_\ell) : E_0(\mathbb{Q}_\ell)].$$

Finally, we state the BSD conjecture:

Conjecture 2.2.3 (The Birch and Swinnerton-Dyer conjecture)**.** Let r_E be the rank of $E(\mathbb{Q})$. Then, the following assertions hold.

1. We have $\mathrm{ord}_{s=1}(L(E, s)) = r_E$.
2. The Tate-Shafarevich group $Ш(E/\mathbb{Q})$ is finite, and

$$\lim_{s \to 1} \frac{L(E, s)}{(s-1)^{r_E} \Omega_E \mathrm{Reg}(E/\mathbb{Q})} = \frac{|Ш(E/\mathbb{Q})| \prod_{\ell | N} m_\ell}{|E(\mathbb{Q})_{\mathrm{tors}}|^2}.$$

The parity of $\mathrm{ord}_{s=1}(L, s)$ is described in terms of the global *root number* of E (cf. [11]). The assertion 1 leads us to the *parity conjecture*:

Conjecture 2.2.4 (The parity conjecture)**.** Let E be an elliptic curve over a number field K and $w(E/K) \in \{\pm 1\}$ its global root number. Then,

$$w(E/K) = (-1)^{\mathrm{rank}(E(K))}.$$

It was shown that the finiteness of Tate-Shafarevich groups implies this conjecture (see [11], [13] for details).

Instead of the rank of the Mordell-Weil group, the p-parity conjecture over K connects the root number with $r_{p^\infty}(E/K) := \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}(K, E[p^\infty]))$. Nekovář [31] proved the p-parity conjecture for most modular elliptic curves for totally real number fields. In [12], T. Dokchitser and V. Dokchitser proved the p-parity conjecture over $\mathbb{Q}$ without any assumption. Namely, they proved the following.

Theorem 2.2.5. *Let E be an elliptic curve over $\mathbb{Q}$. Then, for each prime p,*

$$\mathrm{ord}_{s=1}(L(E, s)) \equiv r_{p^\infty}(E/\mathbb{Q}) \mod 2.$$

Chapter 3

The Mazur-Tate refined conjecture of BSD type

In this chapter, we introduce Mazur-Tate elements, and state the Mazur-Tate refined conjectures of BSD type.

3.1 Modular symbols

Following [29], we recall the modular symbol and its basic properties. We denote by $\mathrm{GL}_2^+(\mathbb{Q})$ the subgroup of $\mathrm{GL}_2(\mathbb{Q})$ consisting of matrices with positive determinant. Let $\mathbb{H}$ denote the upper half-plane in $\mathbb{C}$. For $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$ and $\tau \in \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$, we put

$$A(\tau) = \begin{cases} (a\tau + b)/(c\tau + d) & \text{if } \tau \in \mathbb{H} \cup \mathbb{Q}, \\ a/c & \text{if } \tau = \infty. \end{cases}$$

For a positive integer N, we denote by $\mathscr{S}_2(\Gamma_0(N), \epsilon)$ the space of cusp forms of weight 2 for $\Gamma_0(N)$ with character ϵ. We put $\mathscr{S}_2 = \sum_{N,\epsilon} \mathscr{S}_2(\Gamma_0(N), \epsilon)$.

For $f \in \mathscr{S}_2$ and $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$, we define

$$(f|A)(\tau) = \frac{\det(A)}{(c\tau + d)^2} f\left(\frac{a\tau + b}{c\tau + d}\right).$$

If $A \in \Gamma_0(N)$ and $f \in \mathscr{S}_2(\Gamma_0(N), \epsilon)$, then we have $f|A = \epsilon(d)f$.

For an element $r \in \mathbb{Q} \cup \{\infty\}$ and $f \in \mathscr{S}_2$, we define

$$\phi(f, r) = 2\pi i \int_\infty^r f(z)dz = \begin{cases} 2\pi \int_0^\infty f(r + it)\, dt & \text{if } r \in \mathbb{Q}, \\ 0 & \text{if } r = \infty. \end{cases}$$

Lemma 3.1.1. *For a matrix $A \in \mathrm{GL}_2^+(\mathbb{Q})$, we have*

$$\phi(f|A, r) = \phi(f, A(r)) - \phi(f, A(\infty)).$$

PROOF. We note that $(f|A)(\tau)d\tau = f(A(\tau))d(A(\tau))$. Then, we have

$$\begin{aligned}\phi(f|A, r) &= 2\pi i \int_\infty^r (f|A)(\tau)d\tau = 2\pi i \int_\infty^r f(A(\tau))dA(\tau) = 2\pi i \int_{A(\infty)}^{A(r)} f(z)dz \\ &= 2\pi i \int_\infty^{A(r)} f(z)dz - 2\pi i \int_\infty^{A(\infty)} f(z)dz = \phi(f, A(r)) - \phi(f, A(\infty)).\end{aligned}$$

□

Definition 3.1.2. For rational numbers a, S with $S > 0$ and an element $f \in \mathscr{S}_2$, we define $\lambda(f; a, S)$ by

$$\lambda(f; a, S) = \phi\left(f, -\frac{a}{S}\right) = 2\pi \int_0^\infty f\left(-\frac{a}{S} + it\right) dt.$$

Remark 3.1.3.

1. Comparing the notation of [29] and ours, our $\lambda(f; a, S)$ coincides with $\lambda(f, 1; a, S)$ in [29].
2. If we fix a positive integer S and an element $f \in \mathscr{S}_2$, then $\lambda(f; a, S)$ depends only on a modulo S.

Lemma 3.1.4. *We have*

$$\lambda(f; a, S) = \phi\left(f \left| \begin{bmatrix} 1 & -a \\ 0 & S \end{bmatrix}, 0\right.\right).$$

PROOF. We have

$$\begin{aligned}\phi\left(f \left| \begin{bmatrix} 1 & -a \\ 0 & S \end{bmatrix}, 0\right.\right) &= 2\pi \int_0^\infty f \left| \begin{bmatrix} 1 & -a \\ 0 & S \end{bmatrix} (it)dt = 2\pi \int_0^\infty f\left(\frac{it - a}{S}\right)\frac{dt}{S} \right. \\ &= 2\pi \int_0^\infty f\left(-\frac{a}{S} + it\right) dt \\ &= \lambda(f; a, S).\end{aligned}$$

□

Definition 3.1.5. For every prime ℓ, we define the Hecke operator $T(\ell)$ on $\mathscr{S}_2(\Gamma_0(N), \epsilon)$ as

$$f \mapsto f|T(\ell) := \sum_{u=0}^{\ell-1} f \left| \begin{bmatrix} 1 & u \\ 0 & \ell \end{bmatrix} + \epsilon(\ell) f \right| \begin{bmatrix} \ell & 0 \\ 0 & 1 \end{bmatrix}.$$

Proposition 3.1.6. *For $f \in \mathscr{S}_2(\Gamma_0(N), \epsilon)$ and a prime ℓ, we have*

$$\lambda(f|T(\ell); a, S) = \sum_{u=0}^{\ell-1} \lambda(f; a - uS, \ell S) + \epsilon(\ell)\lambda(f; a, S/\ell).$$

PROOF. For $1 \leq u \leq \ell - 1$, we put $f_u = f \left| \begin{bmatrix} 1 & u \\ 0 & \ell \end{bmatrix} \right.$. By Lemma 3.1.4, we have

$$\begin{aligned}
\lambda(f; a - uS, \ell S) &= \phi\left(f \left| \begin{bmatrix} 1 & uS - a \\ 0 & \ell S \end{bmatrix} \right., 0 \right) \\
&= \phi\left(f \left| \left(\begin{bmatrix} 1 & u \\ 0 & \ell \end{bmatrix} \begin{bmatrix} 1 & -a \\ 0 & S \end{bmatrix} \right) \right., 0 \right) \\
&= \phi\left(f_u \left| \begin{bmatrix} 1 & -a \\ 0 & S \end{bmatrix} \right., 0 \right) \\
&= \lambda(f_u; a, S).
\end{aligned}$$

By Lemma 3.1.4, we also have

$$\begin{aligned}
\lambda(f; a, S/\ell) &= \phi\left(f \left| \begin{bmatrix} 1 & -a \\ 0 & S/\ell \end{bmatrix} \right., 0 \right) \\
&= \phi\left(f \left| \left(\begin{bmatrix} 1 & 0 \\ 0 & 1/\ell \end{bmatrix} \begin{bmatrix} 1 & -a \\ 0 & S \end{bmatrix} \right) \right., 0 \right) \\
&= \lambda\left(f \left| \begin{bmatrix} 1 & 0 \\ 0 & 1/\ell \end{bmatrix} \right.; a, S \right) \\
&= \lambda\left(f \left| \begin{bmatrix} \ell & 0 \\ 0 & 1 \end{bmatrix} \right.; a, S \right).
\end{aligned}$$

By these formulas, we compute the left hand side in the proposition:

$$\begin{aligned}
\sum_{u=0}^{\ell-1} \lambda(f; a - uS, \ell S) + \epsilon(\ell)\lambda(f; a, S/\ell) &= \sum_{u=0}^{\ell-1} \lambda(f_u; a, S) + \epsilon(\ell)\lambda\left(f \left| \begin{bmatrix} \ell & 0 \\ 0 & 1 \end{bmatrix} \right.; a, S \right) \\
&= \lambda\left(\sum_{u=0}^{\ell-1} f_u + \epsilon(\ell) f \left| \begin{bmatrix} \ell & 0 \\ 0 & 1 \end{bmatrix} \right.; a, S \right) \\
&= \lambda\left(\sum_{u=0}^{\ell-1} f_u + \epsilon(\ell) f \left| \begin{bmatrix} \ell & 0 \\ 0 & 1 \end{bmatrix} \right.; a, S \right) \\
&= \lambda(f|T(\ell); a, S).
\end{aligned}$$

□

Definition 3.1.7. For $f \in \mathscr{S}_2(\Gamma_0(N), \epsilon)$, we define $w_N(f) \in \mathscr{S}_2(\Gamma_0(N), \epsilon^{-1})$ by

$$w_N(f)(\tau) = \epsilon(-1) f|A_N = \epsilon(-1)\frac{1}{N\tau^2} f\left(\frac{-1}{N\tau}\right),$$

where $A_N = \begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix}$.

Proposition 3.1.8. *For relatively prime integers a, S such that $S > 0$ and $(S, N) = 1$. We take an integer a' such that $aa'N \equiv -1 \mod S$. Then, we have*

$$\lambda(f; a, S) = -\epsilon(-S)\lambda(w_N(f); a', S).$$

Proof. We put $b = -(Na'a+1)/S$, and then have $-Na'a - bS = 1$, $\epsilon(b) = \epsilon(-S)^{-1}$. Let $W_N = \begin{bmatrix} -Na & b \\ NS & Na' \end{bmatrix}$. Then,

$$A_N \begin{bmatrix} -Na & b \\ NS & Na' \end{bmatrix}^{-1} = \frac{1}{N}\begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix}\begin{bmatrix} Na' & -b \\ -NS & -Na \end{bmatrix} = \begin{bmatrix} S & a \\ Na' & -b \end{bmatrix} \in \Gamma_0(N).$$

Hence, we have

$$w_N(f) = \epsilon(-1) f|A_N = \epsilon(-1) f\left|\begin{bmatrix} S & a \\ Na' & -b \end{bmatrix} W_N = \epsilon(b) f|W_N = \epsilon(-S)^{-1} f|W_N\right.$$

and therefore

$$\lambda(w_N(f); a', S) = \epsilon(-S)^{-1}\lambda(f|W_N; a', S) = \epsilon(-S)^{-1}\phi\left(f\left|W_N\begin{bmatrix} 1 & -a' \\ 0 & S \end{bmatrix}, 0\right.\right). \tag{3.1.1}$$

By Lemma 3.1.1 with $A = A_N$,

$$\phi\left(f\left|W_N\begin{bmatrix} 1 & -a' \\ 0 & S \end{bmatrix} A_N, 0\right.\right) = -\phi\left(f\left|W_N\begin{bmatrix} 1 & -a' \\ 0 & S \end{bmatrix}, 0\right.\right), \tag{3.1.2}$$

where we note $A_N(0) = \infty$ and $A_N(\infty) = 0$. We have

$$W_N\begin{bmatrix} 1 & -a' \\ 0 & S \end{bmatrix} A_N = \begin{bmatrix} -Na & b \\ NS & Na' \end{bmatrix}\begin{bmatrix} -a'N & -1 \\ SN & 0 \end{bmatrix} = N\begin{bmatrix} aa'N + bS & a \\ 0 - S & \end{bmatrix} = N\begin{bmatrix} 1 & -a \\ 0 & S \end{bmatrix}.$$

Then, by (3.1.1) and (3.1.2), we have

$$\begin{aligned} -\epsilon(-S)\lambda(w_N(f); a', S) &= \phi\left(f\left|N\begin{bmatrix} 1 & -a \\ 0 & S \end{bmatrix}, 0\right.\right) = \phi\left(f\left|\begin{bmatrix} 1 & -a \\ 0 & S \end{bmatrix}, 0\right.\right) \\ &= \lambda(f; a, S), \end{aligned}$$

where the second equality follows from Lemma 3.1.1 with $A = \begin{bmatrix} N & 0 \\ 0 & N \end{bmatrix}$, and the last equality follows from Lemma 3.1.4. □

For a cusp form $f(z) = \sum_{n\geq 1} a_n e^{2\pi inz} \in \mathscr{S}_2(\Gamma_0(N), \epsilon)$, we define

$$L(f,s) = \sum_{n\geq 1} \frac{a_n}{n^s},$$

which has an analytic continuation to the whole complex s-plane, and it is known that

$$L(f,s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty f(it) t^s \frac{dt}{t}$$

(see [38, Theorem 3.66] and its proof). Then, we have

$$\lambda(f;0,1) = L(f,1). \tag{3.1.3}$$

Let S be a positive integer and χ a Dirichlet character modulo S. We define

$$\tau_S(\chi) = \sum_{a\in\mathbb{Z}/S\mathbb{Z}} \chi(a)\zeta_S^a,$$

where we put $\zeta_S = \exp(2\pi i/S)$, and $\chi(a) = 0$ if $(a,S) \neq 1$. We put

$$f_\chi(z) = \sum_{n\geq 1} \chi(n) a_n e^{2\pi inz}, \qquad L(f,\chi,s) = L(f_\chi, s) = \sum_{n\geq 1} \frac{\chi(n)a_n}{n^s}.$$

Lemma 3.1.9. *If χ is primitive, then we have*

$$f_{\chi^{-1}}(z) = \frac{1}{\tau_S(\chi)} \sum_{a\in\mathbb{Z}/S\mathbb{Z}} \chi(a) f\left(z + \frac{a}{S}\right).$$

Proof. For $a \in \mathbb{Z}/S\mathbb{Z}$, we have

$$f\left(z+\frac{a}{S}\right) = \sum_{n\geq 1} a_n \zeta_S^{an} e^{2\pi inz}.$$

Thus,

$$\begin{aligned}
\sum_{a\in\mathbb{Z}/SZ} \chi(a) f\left(z+\frac{a}{S}\right) &= \sum_{a\in\mathbb{Z}/SZ} \chi(a) \sum_{n\geq 1} a_n \zeta_S^{an} e^{2\pi inz} = \sum_{n\geq 1} a_n e^{2\pi inz} \sum_{a\in\mathbb{Z}/S\mathbb{Z}} \chi(a)\zeta_S^{an} \\
&= \sum_{n\geq 1} a_n e^{2\pi inz} \chi^{-1}(n) \sum_{a\in\mathbb{Z}/S\mathbb{Z}} \chi(an)\zeta_S^{an} = \tau(\chi) \sum_{n\geq 1} \chi^{-1}(n) a_n e^{2\pi inz} \\
&= \tau(\chi) f_{\chi^{-1}}(z).
\end{aligned}$$

□

Proposition 3.1.10. *If χ is of conductor S, then we have*

$$\tau_S(\chi) L(f, \chi^{-1}, 1) = \sum_{a\in\mathbb{Z}/S\mathbb{Z}} \chi(a)\lambda(f;-a,S).$$

PROOF. By using (3.1.3) and Lemma 3.1.9, we have

$$\begin{aligned} L(f,\chi^{-1},1) = \phi(f_{\chi^{-1}},0) &= \frac{1}{\tau_S(\chi)} \sum_{a\in\mathbb{Z}/S\mathbb{Z}} \chi(a)\phi\left(f\left|\begin{bmatrix}1 & a/S\\ 0 & 1\end{bmatrix},0\right.\right) \\ &= \frac{1}{\tau_S(\chi)} \sum_{a\in\mathbb{Z}/S\mathbb{Z}} \chi(a)\lambda\left(f;-a/S,1\right) \\ &= \frac{1}{\tau_S(\chi)} \sum_{a\in\mathbb{Z}/S\mathbb{Z}} \chi(a)\lambda\left(f;-a,S\right), \end{aligned}$$

where the third equality follows from Lemma 3.1.4. □

3.2 Mazur-Tate elements

In the rest of this chapter, let E be an elliptic curve over $\mathbb{Q}$ of conductor N. We fix a global minimal Weierstrass model of E over $\mathbb{Z}$ and the Néron differential ω. Then, we have a natural map from the first homology group $H_1(E(\mathbb{C}),\mathbb{Z})$ to $\mathbb{C}$

$$H_1(E(\mathbb{C}),\mathbb{Z}) \to \mathbb{C}; \quad \gamma \mapsto \int_\gamma \omega.$$

We denote by Λ the image of this map. Let $\Omega^+, -i\Omega^- > 0$ be the largest numbers such that

$$\Lambda \subseteq \mathbb{Z}\Omega^+ \oplus \mathbb{Z}\Omega^-.$$

We note that Ω^+ does not always coincide with $\Omega_E := \int_{E(\mathbb{R})} |\omega|$ in Section 2.2.

Let $f \in \mathscr{S}_2(\Gamma_0(N))$ be the newform corresponding to E (cf. Theorem 2.2.2). For integers a and S with $S > 0$, we define $[a/S]_E^+, [a/S]_E^- \in \mathbb{R}$ by

$$\lambda(f;-a,S) = \left[\frac{a}{S}\right]_E^+ \Omega^+ + \left[\frac{a}{S}\right]_E^- \Omega^-,$$

that is,

$$2\pi \int_0^\infty f\left(\frac{a}{S}+it\right) dt = \left[\frac{a}{S}\right]_E^+ \Omega^+ + \left[\frac{a}{S}\right]_E^- \Omega^-.$$

By the Manin-Drinfeld theorem ([14], [25]), we have the following:

Proposition 3.2.1. $[a/S]_E^+, [a/S]_E^- \in \mathbb{Q}$.

Since $f(z) \in \mathbb{Q}[[e^{2\pi iz}]]$, we have $f(a/S+it) = \overline{f(-a/S+it)}$ for $t \in \mathbb{R}_{>0}$. Then, we note that

$$\left[-\frac{a}{S}\right]_E^+ = \left[\frac{a}{S}\right]_E^+, \quad \left[-\frac{a}{S}\right]_E^- = -\left[\frac{a}{S}\right]_E^- . \tag{3.2.1}$$

We introduce Mazur-Tate elements.

Definition 3.2.2. For a positive integer S, we put $G_S = \mathrm{Gal}(\mathbb{Q}(\mu_S)/\mathbb{Q})$. We define an element θ_S of $\mathbb{Q}[G_S]$ by

$$\theta_S = \sum_{a \in (\mathbb{Z}/S\mathbb{Z})^\times} \left(\left[\frac{a}{S}\right]_E^+ + \left[\frac{a}{S}\right]_E^- \right) \delta_a \in \mathbb{Q}[G_S],$$

where $\delta_a \in G_S$ is the element satisfying $\delta_a \zeta_S = \zeta_S^a$. We call θ_S the *Mazur-Tate element*.

Remark 3.2.3. Our θ_S slightly differs from the original Mazur-Tate element, which is called the *modular element* in [28]. The image of $\frac{1}{2}\theta_S$ in $\mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\mu_S)^+/\mathbb{Q})]$ is their modular element, where $\mathbb{Q}(\mu_S)^+$ is the maximal totally real subfield of $\mathbb{Q}(\mu_S)$.

For $n|m$, we denote by $\pi_{m/n}$ the map $\mathbb{Q}[G_m] \to \mathbb{Q}[G_n]$ induced by the natural surjection $G_m \to G_n$. We also denote by $\nu_{m,n}$ the map $\mathbb{Q}[G_n] \to \mathbb{Q}[G_m]$ induced by

$$\sigma \mapsto \sum_{\tau \in G_m,\ \tau \mapsto \sigma} \tau \quad \text{for } \sigma \in G_n.$$

Proposition 3.2.4. *Mazur-Tate elements are characterized by the following properties*:

1. *Let S be a positive integer and ℓ a prime. Then, we have*

$$\begin{aligned} \pi_{S\ell/S}\theta_{S\ell} &= -\mathrm{Fr}_\ell(1 - a_\ell \mathrm{Fr}_\ell^{-1} + \epsilon(\ell)\mathrm{Fr}_\ell^{-2})\theta_S \qquad \text{if } \ell \nmid S, \\ \pi_{S\ell/S}\theta_{S\ell} &= a_\ell \theta_S - \epsilon(\ell)\nu_{S,S/\ell}(\theta_{S/\ell}) \qquad \text{if } \ell | S, \end{aligned}$$

   where $a_\ell := a_\ell(E)$ and $\epsilon(\ell)$ are as in Definition 2.2.1*, and Fr_ℓ denotes the arithmetic Frobenius of ℓ.*

2. *For every character χ of G_S with conductor S, we have*

$$\chi(\theta_S) = \tau_S(\chi)\frac{L(E, \chi^{-1}, 1)}{\Omega^\pm},$$

   where $\pm = \chi(-1)$.

Proof. We first prove the assertion 1. For $S > 0$, we put

$$\theta_S^\pm = \sum_{a \in (\mathbb{Z}/S\mathbb{Z})^\times} \left[\frac{a}{S}\right]_E^\pm \delta_a \in \mathbb{Q}[G_S], \quad \Theta_S = \sum_{a \in (\mathbb{Z}/S\mathbb{Z})^\times} \lambda(f; -a, S) \otimes \delta_a \in \mathbb{C}[G_S],$$

and have

$$\begin{aligned} \theta_S &= \theta_S^+ + \theta_S^-, \\ \Theta_S &= \theta_S^+ \Omega^+ + \theta_S^- \Omega^-. \end{aligned} \tag{3.2.2}$$

The map $\pi_{S\ell/S}$ is linearly extended on $\mathbb{C}[G_{S\ell}]$, and we have

$$\pi_{S\ell/S}\left(\Theta_{S\ell}\right) = \pi_{S\ell/S}(\theta^{+}_{S\ell})\Omega^{+} + \pi_{S\ell/S}\theta^{-}_{S\ell}\Omega^{-}. \tag{3.2.3}$$

Then,

(3.2.4)

$$\pi_{S\ell/S}(\Theta_{S\ell}) = \pi_{S\ell/S}\left(\sum_{b\in(\mathbb{Z}/S\ell\mathbb{Z})^{\times}} \lambda(f;-b,S\ell)\otimes\delta_b\right) = \sum_{a\in(\mathbb{Z}/S\mathbb{Z})^{\times}} \sum_{\substack{b\in(\mathbb{Z}/S\ell\mathbb{Z})^{\times}\\ b\mapsto a}} \lambda(f;-b,S\ell)\otimes\delta_a.$$

We suppose that $\ell \nmid S$, and we take integers x, y such that $xS+y\ell = 1$. For an integer a relatively prime to S, we put $e_a = ay\ell$, whose image in $\mathbb{Z}/S\ell\mathbb{Z}$ is a unique element such that

$$e_a \equiv a \mod S, \quad e_a \equiv 0 \mod \ell.$$

Then, by Proposition 3.1.6, we have

$$\begin{aligned}
\sum_{\substack{b\in(\mathbb{Z}/S\ell\mathbb{Z})^{\times}\\ b\equiv a \mod S}} \lambda(f;-b,S\ell) &= \sum_{\substack{b\in(\mathbb{Z}/S\ell\mathbb{Z})\\ b\equiv a \mod S}} \lambda(f;-b,S\ell) - \lambda(f;-e_a,S\ell)\\
&= \sum_{u=0}^{\ell-1} \lambda(f;-a-uS,S\ell) - \lambda(f;-ay,S)\\
&= \lambda(f|T(\ell);-a,S) - \epsilon(\ell)\lambda(f;-a,S/\ell) - \lambda(f;-a\ell^{-1},S)\\
&= a_\ell\lambda(f;-a,S) - \epsilon(\ell)\lambda(f;-a\ell,S) - \lambda(f;-a\ell^{-1},S),
\end{aligned}$$

where the third equality follows from $y\ell \equiv 1 \mod S$. By (3.2.4), we have

$$\begin{aligned}
&\pi_{S\ell/S}(\Theta_{S\ell})\\
=&\sum_{a\in(\mathbb{Z}/S\mathbb{Z})^{\times}} \left(a_\ell\lambda(f;-a,S) - \epsilon(\ell)\lambda(f;-a\ell,S) - \lambda(f;-a\ell^{-1},S)\right)\otimes\delta_a\\
=&\sum_a a_\ell\lambda(f;-a,S)\otimes\delta_a - \epsilon(\ell)\sum_a \lambda(f;-a\ell,S)\otimes\delta_a - \sum_a \lambda(f;-a\ell^{-1},S)\otimes\delta_a\\
=&a_\ell\Theta_S - \epsilon(\ell)\mathrm{Fr}_\ell^{-1}\Theta_S - \mathrm{Fr}_\ell\Theta_S\\
=&-\mathrm{Fr}_\ell^{-1}(1-a_\ell\mathrm{Fr}_\ell+\epsilon(\ell)\mathrm{Fr}_\ell^{-2})\Theta_S\\
=&-\mathrm{Fr}_\ell^{-1}(1-a_\ell\mathrm{Fr}_\ell+\epsilon(\ell)\mathrm{Fr}_\ell^{-2})\theta^{+}_S\Omega^{+} - \mathrm{Fr}_\ell^{-1}(1-a_\ell\mathrm{Fr}_\ell+\epsilon(\ell)\mathrm{Fr}_\ell^{-2})\theta^{-}_S\Omega^{-}.
\end{aligned}$$

By (3.2.3), we obtain

$$\pi_{S\ell/S}(\theta^{\pm}_{S\ell}) = -\mathrm{Fr}_\ell^{-1}(1-a_\ell\mathrm{Fr}_\ell+\epsilon(\ell)\mathrm{Fr}_\ell^{-2})\theta^{\pm}_S,$$

and hence by (3.2.2), we prove the assertion 1 for the case $\ell \nmid S$.

In the case $\ell|S$, for $a \in (\mathbb{Z}/S\mathbb{Z})^\times$ we have

$$\begin{aligned}\sum_{\substack{b\in(\mathbb{Z}/S\ell\mathbb{Z})^\times \\ b\equiv a \mod S}} \lambda(f;-b,S\ell) &= \sum_{u=0}^{\ell-1} \lambda(f;-a-uS,S\ell) \\ &= \lambda(f|T(\ell);-a,S) - \epsilon(\ell)\lambda(f;-a,S/\ell) \\ &= a_\ell \lambda(f;-a,S) - \epsilon(\ell)\lambda(f;-a,S/\ell).\end{aligned}$$

By extending $\nu_{S,S/\ell}$ on $\mathbb{C}[G_{S/\ell}]$ and by (3.2.4), we have

$$\begin{aligned}&\pi_{S\ell/S}(\Theta_{S\ell}) \\ =&\sum_{a\in(\mathbb{Z}/S\mathbb{Z})^\times} (a_\ell\lambda(f;-a,S) - \epsilon(\ell)\lambda(f;-a,S/\ell)) \otimes \delta_a \\ =&\sum_a a_\ell\lambda(f;-a,S)\otimes\delta_a - \epsilon(\ell) \sum_{a\in(\mathbb{Z}/\frac{S}{\ell}\mathbb{Z})^\times} \sum_{\substack{b\in(\mathbb{Z}/S\mathbb{Z})^\times \\ b\mapsto a}} \lambda(f;-a,S/\ell)\otimes\delta_b \\ =&a_\ell\Theta_S - \epsilon(\ell)\nu_{S,S\ell}\Theta_{S/\ell} \\ =&\left(a_\ell\theta_S^+ - \epsilon(\ell)\nu_{S,S\ell}\theta_{S/\ell}^+\right)\Omega^+ + \left(a_\ell\theta_S^- - \epsilon(\ell)\nu_{S,S\ell}(\theta_{S/\ell}^-)\right)\Omega^-.\end{aligned}$$

Hence, by (3.2.3), we obtain

$$\pi_{S\ell/S}(\theta_{S\ell}^\pm) = a_\ell\theta_S^\pm - \epsilon(\ell)\nu_{S,S\ell}(\theta_{S/\ell}^\pm),$$

which implies the assertion 1 for the case $\ell|S$.

We next prove the assertion 2. By Proposition 3.1.10, we have

$$\chi(\Theta_S) = \tau_S(\chi)L(E,\chi^{-1},1).$$

If we put $\pm = \chi(-1)$, then by (3.2.1), we have

$$\chi(\theta_S) = \chi(\theta_S^\pm), \quad \chi(\Theta_S) = \chi(\theta_S^\pm)\Omega^\pm.$$

Hence, we have

$$\chi(\theta_S) = \tau_S(\chi)\frac{L(E,\chi^{-1},1)}{\Omega^\pm}.$$

Finally, we show the uniqueness of $\{\theta_S\}_{S>0}$. We suppose that there exists another $\{\theta'_S\}_{S>0}$ satisfying the assertions 1 and 2. It suffices to show that $\iota_S := \theta_S - \theta'_S$ is zero for each $S>0$. We prove it by induction on the number of divisors of S. If $S=1$, then by the assertion 2, we have $\iota_1 = \theta_1 - \theta'_1 = 0$. For general S, it suffices to show that

$$\chi(\iota_S) = 0 \quad \text{for all Dirichlet characters } \chi \text{ modulo } S,$$

which shows that ι_S belongs to any maximal ideal of $\mathbb{Q}[G_S]$ and hence $\iota_S = 0$. For a primitive character χ, the assertion 2 shows that $\chi(\iota_S) = 0$. For a character χ of conductor $S' < S$, we note that $\chi(\iota_S) = \chi(\pi_{S/S'}(\iota_S))$. By the induction hypothesis and the assertion 1, we have $\pi_{S/S'}(\iota_S) = 0$. Thus, we complete the proof. □

3.3 The refined conjecture

We fix a positive square-free integer S and a subring R of $\mathbb{Q}$ such that $\theta_S \in R[G_S]$ and $|E(\mathbb{Q})_{\mathrm{tors}}| \in R^\times$.

3.3.1 Conjectures on the order of vanishing

In this subsection, we state conjectures which connect θ_S with the Mordell-Weil group or the Selmer group. We denote by I_S the augmentation ideal of $R[G_S]$ and by r_E the rank of $E(\mathbb{Q})$.

Conjecture 3.3.1 (Mazur-Tate)**.** Let $\mathrm{sp}(S)$ denote the number of split multiplicative primes dividing S. Then, we have

$$\theta_S \in I_S^{r_E+\mathrm{sp}(S)}.$$

Remark 3.3.2. It may happen that $\theta_S \in I_S^{r_E+\mathrm{sp}(S)+1}$ (cf. Remark 1.2.2). We note that Bertolini-Darmon [2] proposed a more precise version.

Let χ be a character of G_S, and we put $R[\chi] = R[\mathrm{Im}(\chi)]$. Then, the character χ induces the map $R[G_S] \to R[\chi]$, and we denote by I_χ its kernel. We put

$$r_\chi = \dim_{\mathbb{C}}((E(\mathbb{Q}(\mu_S)) \otimes_{\mathbb{Z}} \mathbb{C})^\chi),$$

where $(E(\mathbb{Q}(\mu_S)) \otimes \mathbb{C})^\chi$ is the subspace of $E(\mathbb{Q}(\mu_S)) \otimes \mathbb{C}$ on which G_S acts by χ. Here, $\sigma \in G_S$ acts on $E(\mathbb{Q}(\mu_S)) \otimes \mathbb{C}$ by $\sigma \otimes 1$.

Conjecture 3.3.3 (Mazur-Tate)**.** We have

$$\theta_S \in I_\chi^{r_\chi}.$$

There is also a conjecture which connects θ_S with the Selmer group as the Iwasawa main conjecture does. By the definition (cf. Subsection 2.1.3) of the Selmer group $\mathrm{Sel}(E/\mathbb{Q}(\mu_S))$, we have an exact sequence

$$0 \to Ш(E/\mathbb{Q}(\mu_S))^\vee \to \mathrm{Sel}(E/\mathbb{Q}(\mu_S))^\vee \to \mathrm{Hom}(E(\mathbb{Q}(\mu_S)) \otimes \mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \to 0,$$

where $\vee$ denotes the Pontryagin dual $\mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$. Let φ denote the map above from $\mathrm{Sel}(E/\mathbb{Q}(\mu_S))^\vee$ to $\mathrm{Hom}(E(\mathbb{Q}(\mu_S)) \otimes \mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$. We note that there is an injective homomorphism

$$\mathrm{Hom}(E(\mathbb{Q}(\mu_S)), \mathbb{Z}) \hookrightarrow \mathrm{Hom}(E(\mathbb{Q}(\mu_S)) \otimes \mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z}); \quad f \mapsto (x \otimes 1/n \mapsto f(x)/n).$$

By this map we regard the finitely generated $\mathbb{Z}[G_S]$-module $\mathrm{Hom}(E(\mathbb{Q}(\mu_S)),\mathbb{Z})$ as a subgroup of $\mathrm{Hom}(E(\mathbb{Q}(\mu_S))\otimes\mathbb{Q}/\mathbb{Z},\mathbb{Q}/\mathbb{Z})$, and put

$$\mathscr{S}(E/\mathbb{Q}(\mu_S)) = \varphi^{-1}(\mathrm{Hom}(E(\mathbb{Q}(\mu_S)),\mathbb{Z})).$$

Then, we have an exact sequence

$$0 \to Ш(E/\mathbb{Q}(\mu_S))^\vee \to \mathscr{S}(E/\mathbb{Q}(\mu_S)) \to \mathrm{Hom}(E(\mathbb{Q}(\mu_S)),\mathbb{Z}) \to 0.$$

We assume that $Ш(E/\mathbb{Q}(\mu_S))$ is finite, and then the module $\mathscr{S}(E/\mathbb{Q}(\mu_S))$ is finitely generated $\mathbb{Z}[G_S]$-module.

Conjecture 3.3.4 (Mazur-Tate)**.** We denote by $\mathrm{Fitt}_{\mathbb{Z}[G_S]}(\mathscr{S}(E/\mathbb{Q}(\mu_S)))$ the 0-th Fitting ideal of the finitely generated $\mathbb{Z}[G_S]$-module $\mathscr{S}(E/\mathbb{Q}(\mu_S))$. Then, we have

$$\theta_S \in \mathrm{Fitt}_{\mathbb{Z}[G_S]}(\mathscr{S}(E/\mathbb{Q}(\mu_S)))\otimes_{\mathbb{Z}} R.$$

Remark 3.3.5. Unlike the Iwasawa main conjecture, it is not generally expected that θ_S generates $\mathrm{Fitt}_{\mathbb{Z}[G_S]}(\mathscr{S}(E/\mathbb{Q}(\mu_S)))\otimes_{\mathbb{Z}} R$. See the remark below [28, Conjecture 3].

Proposition 3.3.6. *Conjecture* 3.3.4 *implies Conjecture* 3.3.3.

Proof. This is [28, Proposition 3]. □

3.3.2 The conjecture on leading coefficients

Mazur-Tate also conjectured a formula on the *leading coefficients* of Mazur-Tate elements. We introduce some notation to review its statement.

In this subsection, we assume Conjecture 3.3.1. For simplicity, we assume that S is relatively prime to N, and denote by $\widetilde{\theta}_S$ the image of $\frac{1}{2}\theta_S$ in $I_{G_S}^{r_E}/I_{G_S^+}^{r_E+1}$, where $G_S^+ := \mathrm{Gal}(\mathbb{Q}(\mu_S)^+/\mathbb{Q})$ and $I_{G_S^+}$ denotes the augmentation ideal of $R[G_S^+]$. We note that our $\widetilde{\theta}_S$ coincides with the leading coefficient considered in [28] (cf. Remark 3.2.3).

For each positive divisor T of S, we denote by j_T the natural map

$$j_T : E(\mathbb{Q}) \to \left(\oplus_{\ell|T} E(\mathbb{F}_\ell)\right) \bigoplus \left(\oplus_{\ell|N} E(\mathbb{Q}_\ell)/E_0(\mathbb{Q}_\ell)\right),$$

and put

$$E_T(\mathbb{Q}) = \ker(j_T), \quad J_T = |\mathrm{coker}(j_T)|.$$

In [28], by modifying ideas of [27], Mazur-Tate defined a canonical paring

$$\langle -,- \rangle_T : E(\mathbb{Q}) \times E_T(\mathbb{Q}) \to G_T^+.$$

We note that $\mathrm{rank}(E_T(\mathbb{Q})) = r_E$. We fix a set $\{P_i\}_{1\le i\le r_E}$ (resp. $\{Q_j\}_{1\le j\le r_E}$) of elements of $E(\mathbb{Q})$ (resp. $E_T(\mathbb{Q})$) which is a $\mathbb{Z}$-basis of $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$ (resp. $E_T(\mathbb{Q})/E_T(\mathbb{Q})_{\mathrm{tors}}$). More precisely, we need to choose elements above with *compatible orientations* of $E(\mathbb{Q})\otimes\mathbb{R}$ (see [28, §2.5] for the detail) in order to remove an ambiguity up to sign in the definition of the discriminant d_T below. We simply regard G_T^+ as a $\mathbb{Z}$-module, and denote by $\mathrm{Sym}_{\mathbb{Z}}(G_T^+)$ the symmetric algebra $\bigoplus_{i=0}^{\infty}\mathrm{Sym}^i(G_T^+)$. Then, we note that $\langle P_i, Q_j\rangle_T \in \mathrm{Sym}^1(G_T^+)$, and regard $(\langle P_i, Q_j\rangle_T)_{1\le i,j\le r_E}$ as a matrix with coefficients in $\mathrm{Sym}_{\mathbb{Z}}(G_T^+)$, whose determinant belongs to $\mathrm{Sym}^{r_E}(G_T^+)$. We define d_T by

$$d_T = \frac{1}{[E(\mathbb{Q}) : \oplus_{1\le i\le r}\mathbb{Z}P_i][E_T(\mathbb{Q}) : \oplus_{1\le j\le r}\mathbb{Z}Q_j]} \otimes \det\left(\langle P_i, Q_j\rangle_T\right) \in R\otimes_{\mathbb{Z}}\mathrm{Sym}^{r_E}(G_T^+),$$

which is independent of the choice of $\{P_i\}$ and $\{Q_j\}$. Here we use the assumption $|E(\mathbb{Q})_{\mathrm{tors}}| \in R^\times$. Let η_{r_E} denote the morphism from $R\otimes_{\mathbb{Z}}\mathrm{Sym}^{r_E}(G_T^+)$ to $I_{G_T^+}^{r_E}/I_{G_T^+}^{r_E+1}$ induced by the natural homomorphism $G_T^+ \to I_{G_T^+}/I_{G_T^+}^2;\ \sigma\mapsto\sigma-1$.

We note that there is a natural exact sequence

$$\prod_{\ell|\frac{S}{T}} G_\ell \to G_S^+ \xrightarrow{\pi_{S/T}} G_T^+ \to 0.$$

For each $g_T \in G_T^+$, we take its lift g_S to G_S^+. If we put $h_T = \prod_{\ell|\frac{S}{T}}|G_\ell|$, then

$$\mu_{S,T}(g_T) = g_S^{h_T}$$

is independent of the choice of g_S. Then, we have a homomorphism $\mu_{S,T} : G_T^+ \to G_S^+$. The following is the conjecture on the leading coefficient $\widetilde{\theta}_S$:

Conjecture 3.3.7 (Mazur-Tate)**.** We assume that S is relatively prime to N and the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ is finite. Then, the element θ_S belongs to $I_S^{r_E}$ and

$$\widetilde{\theta}_S = |Ш(E/\mathbb{Q})|\cdot\sum_{T|S>0}(-1)^{\nu(T)}J_T\cdot\eta_{r_E}\left(\mu_{S,T}(d_T)\right) \in I_{G_S^+}^{r_E}/I_{G_S^+}^{r_E+1},$$

where $\nu(T)$ denotes the number of primes dividing T.

Remark 3.3.8.

1. It may happen that $\eta_{r_E}(d_S) = 0$. Bertolini-Darmon [2] constructed a lift of $\eta_{r_E}(d_S)$ to $I_{G_S^+}^{r_E}$, which gives extra information when $\eta_{r_E}(d_S) = 0$.
2. See [28, Conjecture 4] for more general cases. Although Conjecture 3.3.7 might look different from the original conjecture [28, Conjecture 4], it is not difficult to check that they are equivalent.

Chapter 4

Divisibility of Euler systems for elliptic curves

In this chapter, by modifying Darmon's argument in [8], we show that some Darmon-Kolyvagin derivatives of Euler systems are divisible by a power of p (Theorem 4.3.10). By using this divisibility, we obtain Corollary 4.3.13, which is a key to proving our main result (Theorem 5.4.1).

Throughout this chapter, we fix a prime $p \geq 5$. For a positive integer S, we denote by $\mathbb{Q}(S)$ the maximal p-extension of $\mathbb{Q}$ inside $\mathbb{Q}(\mu_S)$ and put $\Gamma_S = \mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q})$. Let I_S be the augmentation ideal of $\mathbb{Z}_p[\Gamma_S]$. For relatively prime integers m, n, by the canonical decomposition $\Gamma_{mn} = \Gamma_m \times \Gamma_n$, we regard Γ_m and Γ_n as subgroups of Γ_{mn}

4.1 Darmon-Kolyvagin derivatives

Following [8], we introduce derivatives which we call Darmon-Kolyvagin derivatives as in [24]. The reason why we consider them is explained in Lemma 4.1.8.

As usual, for integers $j \geq 0$ and $k \geq 1$, we put

$$\binom{j}{k} = \frac{j(j-1)\cdots(j-k+1)}{k!}.$$

We put $\binom{j}{0} = 1$ for $j \geq 0$.

For an element $\sigma \in \Gamma_S$ of order n and for an integer $k \geq 0$, we define

$$D_\sigma^{(k)} = \sum_{j=0}^{n-1} \binom{j}{k} \sigma^j \in \mathbb{Z}[\Gamma_S].$$

We note that $D_\sigma^k = 0$ if $k \geq n$. For $k < 0$, we define $D_\sigma^k = 0$. We recall its basic property.

Lemma 4.1.1. *If $\sigma \in \Gamma_S$ is of order n and $1 \leq k \leq n-1$, then*

$$(\sigma - 1)D_\sigma^k = \binom{n}{k} - \sigma D_\sigma^{k-1}.$$

In particular, if n is a power q of p and $0 < k < p$, then we have

$$(\sigma - 1)D_\sigma^k \equiv -\sigma D_\sigma^{k-1} \mod q.$$

Proof. We have

$$\begin{aligned}
(\sigma-1)D_\sigma^k &= \sum_{j=0}^{n-1}\binom{j}{k}\sigma^{j+1} - \sum_{j=0}^{n-1}\binom{j}{k}\sigma^j = \sum_{j=1}^{n}\binom{j-1}{k}\sigma^j - \sum_{j=0}^{n}\binom{j}{k}\sigma^j + \binom{n}{k} \\
&= \binom{n}{k} + \sum_{j=1}^{n}\left(\binom{j-1}{k} - \binom{j}{k}\right)\sigma^j - \binom{0}{k} \overset{(*)}{=} \binom{n}{k} - \sum_{j=1}^{n}\binom{j-1}{k-1}\sigma^j \\
&= \binom{n}{k} - \sigma\sum_{j=1}^{n}\binom{j-1}{k-1}\sigma^{j-1} = \binom{n}{k} - \sigma\sum_{j=0}^{n-1}\binom{j}{k-1}\sigma^j \\
&= \binom{n}{k} - \sigma D_\sigma^{k-1},
\end{aligned}$$

where the equation $(*)$ follows from $\binom{0}{k} = 0$ and from

$$\begin{aligned}
\binom{j-1}{k} - \binom{j}{k} &= \frac{(j-1)(j-2)\cdots(j-k+1)(j-k)}{k!} - \frac{j(j-1)\cdots(j-k+1)}{k!} \\
&= \frac{(j-1)(j-2)\cdots(j-k+1)(j-k-j)}{k!} \\
&= -\frac{(j-1)(j-2)\cdots(j-k+1)k}{k(k-1)!} \\
&= -\frac{(j-1)(j-2)\cdots(j-k+1)}{(k-1)!} = -\binom{j-1}{k-1}.
\end{aligned}$$

□

Definition 4.1.2. In the following, we fix a generator σ_ℓ of Γ_ℓ for each prime ℓ, and write $D_\ell^{(k)} = D_{\sigma_\ell}^{(k)}$. Let $S > 0$ be a square-free integer. We call an element D of $\mathbb{Z}[\Gamma_S]$ a *Darmon-Kolyvagin derivative*, or simply, a derivative if D is of the following form:

$$D_{\ell_1}^{(k_1)} \cdots D_{\ell_s}^{(k_s)} \in \mathbb{Z}[\Gamma_{\ell_1 \cdots \ell_s}] \subset \mathbb{Z}[\Gamma_S],$$

where $\ell_1, \ldots, \ell_s$ are distinct primes dividing S, and $k_1, \ldots, k_s$ are integers such that $0 \leq k_i < |\Gamma_{\ell_i}|$ for each i. We note that $\ell_1, \ldots, \ell_s, k_1, \ldots, k_s$ are uniquely determined. We define

$$\mathrm{Supp}(D) = \ell_1 \cdots \ell_s, \qquad \mathrm{Cond}(D) = \prod_{k_i > 0} \ell_i,$$

which we call the *support* and the *conductor* of D, respectively. We put

$$\mathrm{ord}(D) = k_1 + \cdots + k_s, \quad n(D) = \min_{k_i>0}\{|\Gamma_{\ell_i}|\}, \quad e_{\ell_i}(D) = k_i.$$

We call $n(D)$ the *order* of D. Since Γ_ℓ is a p-group for each prime ℓ, the natural number $n(D)$ is a power of p. When $k_i = 0$ for all i, we define $n(D) = 1$. When $S = \ell_1 \cdots \ell_s$, we define the norm operator as

$$N_S = D^{(0)}_{\ell_1} \cdots D^{(0)}_{\ell_s}.$$

Remark 4.1.3. In the original argument on Euler systems by Kolyvagin [20], the derivatives of the form $D^{(1)}_{\ell_1} \cdots D^{(1)}_{\ell_s}$ are used.

Example 4.1.4. Let S be a positive square-free integer and $S = \ell_1 \cdots \ell_s$ its prime factorization.

1. $\mathrm{Supp}(D^{(2)}_{\ell_1} \cdots D^{(2)}_{\ell_{s-1}}) = \mathrm{Cond}(D^{(2)}_{\ell_1} \cdots D^{(2)}_{\ell_{s-1}}) = \dfrac{S}{\ell_s}$,
2. $\mathrm{Supp}(D^{(2)}_{\ell_1} \cdots D^{(2)}_{\ell_{s-1}} D^{(0)}_{\ell_s}) = S, \ \ \mathrm{Cond}(D^{(2)}_{\ell_1} \cdots D^{(2)}_{\ell_{s-1}} D^{(0)}_{\ell_s}) = \dfrac{S}{\ell_s}$.

Let S be a square-free integer $S > 0$ and M a $\mathbb{Z}_p[\Gamma_S]$-module without p-torsion. We take an element $a \in M$, and put

$$\theta = \sum_{\gamma \in \Gamma_S} \gamma a \otimes \gamma \in M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\Gamma_S].$$

The element θ has a *Taylor expansion* as follows.

Proposition 4.1.5. *Let $S = \ell_1 \cdots \ell_s$ be the prime factorization of S. Then, we have*

$$\theta = \sum_{\underline{k}=(k_1,\ldots,k_s) \in \mathbb{Z}^{\oplus s}_{\geq 0}} D_{\underline{k}} a \otimes (\sigma_{\ell_1} - 1)^{k_1} \cdots (\sigma_{\ell_s} - 1)^{k_s},$$

where $D_{\underline{k}} := D^{(k_1)}_{\ell_1} \cdots D^{(k_s)}_{\ell_s}$ for $\underline{k} = (k_1, \ldots, k_s)$.

Remark 4.1.6. Since $D^{(k_i)}_{\ell_i} = 0$ if $k_i \geq |\Gamma_{\ell_i}|$, we have $D_{\underline{k}} = 0$ for all but finitely many $\underline{k} \in \mathbb{Z}^{\oplus s}_{\geq 0}$

Proof. We prove the proposition by induction on the number of primes dividing S,

We first assume that S is a prime ℓ and put $\sigma = \sigma_\ell$. Since Γ_ℓ is generated by σ, we have

$$\theta = \sum_{j=0}^{|\Gamma_\ell|-1} \sigma^j a \otimes \sigma^j.$$

For each j, we note that

$$\sigma^j = (\sigma - 1 + 1)^j = \sum_{k=0}^{j} \binom{j}{k} (\sigma - 1)^k = \sum_{k \geq 0} \binom{j}{k} (\sigma - 1)^k.$$

Hence, we have

$$\begin{aligned}\sum_{j=0}^{|\Gamma_\ell|-1} \sigma^j a \otimes \sigma^j &= \sum_{j=0}^{|\Gamma_\ell|-1} \sigma^j a \otimes \sum_{k \geq 0} \binom{j}{k} (\sigma - 1)^k = \sum_{j=0}^{|\Gamma_\ell|-1} \sum_{k \geq 0} \binom{j}{k} \sigma^j a \otimes (\sigma - 1)^k \\ &= \sum_{k \geq 0} \sum_{j=0}^{|\Gamma_\ell|-1} \binom{j}{k} \sigma^j a \otimes (\sigma - 1)^k = \sum_{k \geq 0} D_\ell^{(k)} a \otimes (\sigma - 1)^k.\end{aligned}$$

Then, we complete the case where S is a prime.

In the general case, we put $T = S/\ell_1$. Then, we have

$$\theta = \sum_{\gamma_1 \in \Gamma_{\ell_1}} \sum_{\gamma \in \Gamma_T} \gamma_1 \gamma a \otimes \gamma \gamma_1.$$

By the induction hypothesis,

$$\sum_{\gamma \in \Gamma_T} \gamma a \otimes \gamma = \sum_{\underline{k}' = (k_2, \ldots, k_s) \in \mathbb{Z}_{\geq 0}^{\oplus s-1}} D_{\underline{k}'} a \otimes (\sigma_{\ell_2} - 1)^{k_2} \cdots (\sigma_{\ell_s} - 1)^{k_s}.$$

Hence, we have

$$\begin{aligned}\theta &= \sum_{\gamma_1 \in \Gamma_{\ell_1}} \sum_{\gamma \in \Gamma_T} \gamma_1 \gamma a \otimes \gamma \gamma_1 \\ &= \sum_{\gamma_1 \in \Gamma_{\ell_1}} \sum_{\underline{k}' = (k_2, \ldots, k_s) \in \mathbb{Z}_{\geq 0}^{\oplus s-1}} \gamma_1 D_{\underline{k}'} a \otimes (\sigma_{\ell_2} - 1)^{k_2} \cdots (\sigma_{\ell_s} - 1)^{k_s} \gamma_1 \\ &= \sum_{\underline{k}'} D_{\underline{k}'} \sum_{\gamma_1 \in \Gamma_{\ell_1}} \gamma_1 a \otimes \gamma_1 (\sigma_{\ell_2} - 1)^{k_2} \cdots (\sigma_{\ell_s} - 1)^{k_s} \\ &\overset{(*)}{=} \sum_{\underline{k}'} D_{\underline{k}'} \sum_{k_1 \geq 0} \left(D_{\ell_1}^{(k_1)} a \otimes (\sigma_{\ell_1} - 1)^{k_1} \right) (\sigma_{\ell_2} - 1)^{k_2} \cdots (\sigma_{\ell_s} - 1)^{k_s} \\ &= \sum_{\underline{k} = (k_1, \ldots, k_s) \in \mathbb{Z}_{\geq 0}^{\oplus s}} D_{\underline{k}} a \otimes (\sigma_{\ell_1} - 1)^{k_1} \cdots (\sigma_{\ell_s} - 1)^{k_s},\end{aligned}$$

where the equality $(*)$ also follows from the induction hypothesis. Thus, we complete the proof. □

Lemma 4.1.7. *Let G be a finite abelian p-group and σ an element of G with order q. Then, we have*

$$q(\sigma - 1) \in I_G^p,$$

where I_G denotes the augmentation ideal of $\mathbb{Z}_p[G]$.

PROOF. We have

$$0 = \sigma^q - 1 = (\sigma - 1 + 1)^q - 1 = \sum_{k=1}^{q} \binom{q}{k} (\sigma - 1)^k$$
$$= q(\sigma - 1)\left(1 + \sum_{k=2}^{p-1} \frac{1}{q}\binom{q}{k}(\sigma - 1)^{k-1}\right) + \sum_{k=p}^{q} \binom{q}{k}(\sigma - 1)^k,$$

and hence

$$q(\sigma - 1)\left(1 + \sum_{k=2}^{p-1} \frac{1}{q}\binom{q}{k}(\sigma - 1)^{k-1}\right) = -\sum_{k=p}^{q} \binom{q}{k}(\sigma - 1)^k \in I_G^p. \tag{4.1.1}$$

Since q is a power of p, we have $\frac{1}{q}\binom{q}{k} \in \mathbb{Z}$ if $1 \leq k \leq p-1$. We note that $\mathbb{Z}_p[G]$ is a local ring whose maximal ideal is $p\mathbb{Z}_p[G] + I_G$, and hence

$$1 + \sum_{k=2}^{p-1} \frac{1}{q}\binom{q}{k}(\sigma - 1)^{k-1} \in \mathbb{Z}_p[G]^\times.$$

Thus, by (4.1.1), we conclude $q(\sigma - 1) \in I_G^p$. □

Combining Proposition 4.1.5 and Lemma 4.1.7, we have the following.

Lemma 4.1.8. *Let $t \geq 1$. Assume that for all Darmon-Kolyvagin derivatives such that $\mathrm{Supp}(D) = S$ and $\mathrm{ord}(D) < \min\{t, p\}$, we have $Da \equiv 0 \mod n(D)$. Then,*

$$\theta - N_S a \otimes 1 \in M \otimes_{\mathbb{Z}_p} I_S^{\min\{t,p\}}.$$

Remark 4.1.9. This is [8, Lemma 3.8]. It seems that there is an error in the statement of [8, Lemma 3.8]. However, the error is not crucial when we consider Euler systems.

PROOF. As in Proposition 4.1.5, we write

$$\theta = \sum_{\underline{k}=(k_1,\dots,k_s)\in\mathbb{Z}_{\geq 0}^{\oplus s}} D_{\underline{k}} a \otimes (\sigma_{\ell_1} - 1)^{k_1} \cdots (\sigma_{\ell_s} - 1)^{k_s}. \tag{4.1.2}$$

We pick $\underline{k} = (k_1, \dots, k_s) \in \mathbb{Z}_{\geq 0}^{\oplus s} \setminus \{0, \dots, 0\}$ such that $k_1 + \cdots k_s < \min\{t, p\}$. In other words, $\mathrm{ord}(D_{\underline{k}}) < \min\{t, p\}$. By the definition of $n(D_{\underline{k}})$, we have $|\Gamma_{\ell_i}| = n(D_{\underline{k}})$ and $k_i > 0$ for some i. Then, Lemma 4.1.7 shows that $n(D_{\underline{k}})(\sigma_{\ell_i} - 1) \in I_S^p$. Hence, since $D_{\underline{k}} a \equiv 0 \mod n(D_{\underline{k}})$, we have

$$D_{\underline{k}} a \otimes (\sigma_{\ell_1} - 1)^{k_1} \cdots (\sigma_{\ell_s} - 1)^{k_s} \in M \otimes I_S^p. \tag{4.1.3}$$

This holds for each $D_{\underline{k}}$ such that $\mathrm{ord}(D_{\underline{k}}) < \min\{t, p\}$ and $D_{\underline{k}} \neq N_S$. By (4.1.2), we complete the proof. □

Remark 4.1.10. Under the assumption of the lemma, we also have

$$\sum_{\sigma} \sigma^{-1} a \otimes \sigma - N_S a \otimes 1 \in M \otimes I_S^{\min\{t,p\}}$$

by twisting the action of Γ_S on M.

4.2 Euler systems and their local behavior at primes not dividing p

In this section, following [36, Chapter 4], we study local behavior of Darmon-Kolyvagin derivatives of Euler systems at primes *not* dividing p. While Rubin [36] considers Euler systems for general Galois representations, we only consider Euler systems for elliptic curves.

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N without complex multiplication. We denote by T the p-adic Tate module $T_p(E)$ of E.

4.2.1 Preliminaries on Galois cohomology

In this subsection, we review basic results on Galois cohomology. We assume that the p-adic representation

$$\rho : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_p}(T)$$

is surjective. In particular, the Galois representation $G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_p}(E[p])$ is surjective, and then the module $E[p]$ is irreducible as a $G_{\mathbb{Q}}$-module.

Proposition 4.2.1. *For a power q of p and a finite abelian extension F of $\mathbb{Q}$, we have $E(F)[q] = 0$. Moreover, the restriction map induces an isomorphism*

$$H^1(\mathbb{Q}, E[q]) \cong H^0\left(F/\mathbb{Q}, H^1(F, E[q])\right).$$

Proof. For the first assertion, it suffices to show that $E(F)[p] = 0$. We assume that $E(F)[p] \neq 0$, and take a non-trivial point $P \in E(F)[p]$. Since the Galois representation $G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}/p\mathbb{Z}}(E[p])$ is surjective, for each non-trivial point $Q \in E[p]$ there exists an element $\sigma \in G_{\mathbb{Q}}$ such that $\sigma P = Q$. Since the extension $F/\mathbb{Q}$ is a Galois extension, we have $Q \in E(F)[p]$. Thus, $\mathbb{Q}(E[p]) \subseteq F$, which implies that $\mathrm{Gal}(\mathbb{Q}(E[q])/\mathbb{Q})$ is abelian. However, since $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is not abelian, we have a contradiction. Then, we show that $E(F)[q] = 0$.

By the five term exact sequence (cf. [32, Proposition 1.6.7]), we have an exact sequence

$$0 \to H^1(F/K, E(F)[q]) \to H^1(\mathbb{Q}, E[q]) \to H^0\left(F/\mathbb{Q}, H^1(F, E[q])\right) \to H^2(F/\mathbb{Q}, E(F)[q]).$$

Since $E(F)[q] = 0$, we conclude the latter assertion of the proposition. □

Proposition 4.2.2. *Let L be the filed $\mathbb{Q}(E[q])$ for a power q of p. Then. we have*

$$H^1(L/\mathbb{Q}, E[q]) = 0.$$

PROOF. Since the Galois representation $G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}/q\mathbb{Z}}(E[q])$ is surjective, we have $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$. If we fix a $\mathbb{Z}/q\mathbb{Z}$-isomorphism $E[q] \cong (\mathbb{Z}/q\mathbb{Z})^{\oplus 2}$, then

$$H^1(L/\mathbb{Q}, E[q]) \cong H^1(\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}), (\mathbb{Z}/q\mathbb{Z})^{\oplus 2}),$$

where the action of $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$ on $(\mathbb{Z}/q\mathbb{Z})^{\oplus 2}$ is the natural action. By the inflation-restriction exact sequence, we have an exact sequence

$$\begin{aligned} 0 \to H^1\left(\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})/\{\pm 1\}, H^0\left(\{\pm 1\}, (\mathbb{Z}/q\mathbb{Z})^{\oplus 2}\right)\right) \\ \to H^1(\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}), (\mathbb{Z}/q\mathbb{Z})^{\oplus 2}) \to H^1(\{\pm 1\}, (\mathbb{Z}/q\mathbb{Z})^{\oplus 2})), \end{aligned}$$

where we put $-1 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$. Then, we are reduced to showing that

$$H^0\left(\{\pm 1\}, (\mathbb{Z}/q\mathbb{Z})^{\oplus 2}\right) = H^1\left(\{\pm 1\}, (\mathbb{Z}/q\mathbb{Z})^{\oplus 2}\right) = 0.$$

For $a, b \in \mathbb{Z}/q\mathbb{Z}$, we have

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} -a & 0 \\ 0 & -b \end{bmatrix}.$$

Since $p \neq 2$, this implies that $H^0\left(\{\pm 1\}, (\mathbb{Z}/q\mathbb{Z})^{\oplus 2}\right) = 0$. Since the order of $\{\pm 1\}$ is 2, we also have $H^1\left(\{\pm 1\}, (\mathbb{Z}/q\mathbb{Z})^{\oplus 2}\right) = 0$. □

Proposition 4.2.3. *There exists an element $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{p^\infty}))$ such that*

$$T/(\tau - 1)T \cong \mathbb{Z}_p. \tag{4.2.1}$$

PROOF. We recall that the Weil pairing induces an isomorphism $\det_{\mathbb{Z}_p}(T) \cong \varprojlim \mu_{p^n}$. Hence, if we fix a $\mathbb{Z}_p$-isomorphism $T \cong \mathbb{Z}_p^{\oplus 2}$, then the Galois representation induces the surjective map $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{p^\infty})) \to \mathrm{SL}_2(\mathbb{Z}_p)$. We take an element $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{p^\infty}))$ such that $\rho(\tau) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, and conclude (4.2.1). □

For a torsion module M and an element $b \in M$, we denote by $\mathrm{ord}(b, M)$ the order of b.

Lemma 4.2.4. *Let q be a power of p and L a finite Galois extension of $\mathbb{Q}$ such that G_L acts trivially on $E[q]$. Then for $\kappa, \eta \in H^1(\mathbb{Q}, E[q])$, there exists an element γ of G_L such that*

1. $\mathrm{ord}\left(\kappa(\gamma\tau), E[q]/(\tau - 1)E[q]\right) \geq \mathrm{ord}(\kappa, H^1(L, E[q]))$,
2. $\mathrm{ord}\left(\eta(\gamma\tau), E[q]/(\tau - 1)E[q]\right) \geq \mathrm{ord}(\eta, H^1(L, E[q]))$,

where τ is as in (4.2.1), and we regard κ, η as elements of $H^1(L, E[q])$ by the restriction map $H^1(\mathbb{Q}, E[q]) \to H^1(L, E[q])$.

Remark 4.2.5. For $\gamma \in G_L$ and $\kappa \in H^1(\mathbb{Q}, E[q])$, the image of $\kappa(\gamma\tau)$ in $E[q]/(\tau-1)E[q]$ is independent of the choice of a cocycle representing κ. Indeed, if we take a coboundary x given by $\sigma \mapsto (\sigma - 1)P$ for some $P \in E[q]$, then for $\gamma \in G_L$ we have

$$x(\gamma\tau) = (\gamma\tau - 1)P = (\tau - 1)P \in (\tau - 1)E[q].$$

Proof. We follow the proof of [36, Lemma 5.2.1]. We define subsets of G_L

$$B_\kappa = \{\gamma \in G_L;\ \mathrm{ord}(\kappa(\gamma\tau), E[q]/(\tau-1)E[q]) < \mathrm{ord}(\kappa, H^1(L, E[q]))\},$$
$$B_\eta = \{\gamma \in G_L;\ \mathrm{ord}(\eta(\gamma\tau), E[q]/(\tau-1)E[q]) < \mathrm{ord}(\eta, H^1(L, E[q]))\}.$$

Since each $\gamma \in G_L \setminus (B_\kappa \cup B_\eta)$ satisfies the inequalities 1,2 of the lemma, we are reduced to showing that $B_\kappa \cup B_\eta$ is a proper subset of G_L. We define a subgroup J of G_L by

$$J = \{\gamma \in G_L;\ \mathrm{ord}(\kappa(\gamma), E[q]/(\tau-1)E[q]) < \mathrm{ord}(\kappa, H^1(L, E[q]))\}.$$

Then, $B_\kappa = \emptyset$ or $B_\kappa = \sigma J$ for some $\sigma \in G_L$. To prove this, we assume that $B_\kappa \neq \emptyset$, and we fix an element $\sigma \in B_\kappa$. Let $\delta \in B_\kappa$. Then, we have

$$\kappa(\sigma^{-1}\delta\tau) \equiv \kappa(\sigma^{-1}\delta) + \kappa(\tau) \mod (\tau - 1)E[q],$$

and hence

$$\begin{aligned}\kappa(\sigma^{-1}\delta) &\equiv \kappa(\sigma^{-1}\delta\tau) - \kappa(\tau) \equiv \sigma^{-1}\kappa(\delta\tau) + \kappa(\sigma^{-1}) - \kappa(\tau) \equiv \kappa(\delta\tau) - \kappa(\sigma) - \kappa(\tau) \\ &\equiv \kappa(\delta\tau) - \kappa(\sigma\tau) \mod (\tau - 1)E[q],\end{aligned} \tag{4.2.2}$$

where the third congruence follows from the assumption that G_L acts on $E[q]$ trivially and $H^1(L, E[q]) = \mathrm{Hom}(G_L, E[q])$. Since $\sigma, \delta \in B_\kappa$, (4.2.2) shows that $\sigma^{-1}\delta \in J$, and hence $\delta \in \sigma J$. Conversely, we take $\sigma g \in \sigma J$. Then, we have

$$\begin{aligned}\kappa(\sigma g\tau) &\equiv \sigma\kappa(g\tau) + \kappa(\sigma) \equiv \kappa(g\tau) + \kappa(\sigma) \equiv g\kappa(\tau) + \kappa(g) + \kappa(\sigma) \\ &\equiv \kappa(g) + \kappa(\sigma) + \kappa(\tau) \equiv \kappa(g) + \kappa(\sigma\tau) \mod (\tau - 1)E[q],\end{aligned}$$

which implies that $\sigma g \in B_\kappa$. Thus, we deduce that $B_\kappa = \emptyset$ or $B = \sigma J$ for some $\sigma \in G_L$.

We put $d = \mathrm{ord}(\kappa, \mathrm{Hom}(G_L, E[q]))$. Since $\kappa \in \mathrm{Hom}(G_L, E[q])^{\mathrm{Gal}(L/\mathbb{Q})}$, we have

$$h(\kappa(\gamma)) = \kappa(h\gamma h^{-1}) \quad \text{for } \gamma \in G_L,\ h \in G_{\mathbb{Q}}.$$

Therefore, $\kappa(G_L)$ is a $G_{\mathbb{Q}}$-stable subgroup of $E[p^d]$ which is not contained in $E[p^{d-1}]$. Since $p^{d-1}\kappa(G_L)$ is a $G_{\mathbb{Q}}$-stable subgroup of $E[p]$ and $E[p]$ is irreducible as a $G_{\mathbb{Q}}$-module,

we have $p^{d-1}\kappa(G_L) = E[p]$, and hence $\kappa(G_L) = E[p^d]$. By the definition of $J \subseteq G_L$, we have

$$\kappa(J) \subseteq \big(E[p^{d-1}] + (\tau-1)E[q]\big) \cap \kappa(G_L) = \big(E[p^{d-1}] + (\tau-1)E[q]\big) \cap E[p^d].$$

Since $E[q]/(\tau-1)E[q] \cong \mathbb{Z}/q\mathbb{Z}$, we have $(\tau-1)E[q] \cong Z/q\mathbb{Z}$, and hence

$$\big(E[p^{d-1}] + (\tau-1)E[q]\big) \cap E[p^d] \subsetneq E[p^d] = \kappa(G_L).$$

Then, we obtain $\kappa(J) \subsetneq \kappa(G_L)$, and hence $[G_L : J] \geq p$.

In the same way, we deduce that B_η is either empty or a coset of a subgroup of G_L of index at least p. Since $p > 2$, we have $B_\kappa \cup B_\eta \neq G_L$. □

4.2.2 Euler systems

We fix notation on Euler systems. We put

$$\begin{aligned}\mathscr{R} &= \{\text{primes not dividing } pN\},\\ \mathscr{N} &= \{\text{square-free products of primes in } \mathscr{R}\} \cup \{1\}.\end{aligned}$$

For each prime $\ell \in \mathscr{R}$, we define $P_\ell(t)$ by

$$P_\ell(t) = 1 - a_\ell t + t^2 \in \mathbb{Z}[t], \tag{4.2.3}$$

where $a_\ell := a_\ell(E)$ is as in Definition 2.2.1.

Definition 4.2.6. We call a system $\{z_{Sp^n}\}_{S\in\mathscr{N},n\geq 0} \in \prod_{S,n} H^1(\mathbb{Q}(Sp^n), T)$ an (modified) *Euler system* for T if $\{z_{Sp^n}\}$ satisfies the following conditions.

1. For $S \in \mathscr{N}$, a prime $\ell \in \mathscr{R}$ not dividing S, and $n \geq 0$, we have

   $$\mathrm{Cor}_{S\ell/S} z_{S\ell p^n} = P_\ell(\mathrm{Fr}_\ell^{-1}) z_{Sp^n},$$

   where $\mathrm{Cor}_{S\ell p^n/Sp^n} : H^1(\mathbb{Q}(S\ell p^n), T) \to H^1(\mathbb{Q}(Sp^n), T)$ denotes the corestriction map, and $\mathrm{Fr}_\ell \in \Gamma_{Sp^n}$ denotes the arithmetic Frobenius at ℓ.

2. For $S \in \mathscr{N}$, the system $\{z_{Sp^n}\}_{n\geq 0}$ is a norm compatible system, that is,

   $$\{z_{Sp^n}\}_{n\geq 0} \in \varprojlim H^1(\mathbb{Q}(Sp^n), T),$$

   where the limit is taken with respect to the corestriction maps $\mathrm{Cor}_{Sp^{n+1}/Sp^n}$.

Remark 4.2.7. Our definition of Euler system slightly differs from the usual definition of Kato [17], Perrin-Riou [35] and Rubin [36]. In their definition, instead of the condition 1 in Definition 4.2.6, each Euler system is required to satisfy

$$\mathrm{Cor}_{S\ell p^n/Sp^n}(z_{S\ell p^n}) = \left(1 - \frac{a_\ell}{\ell}\mathrm{Fr}_\ell^{-1} + \frac{1}{\ell}\mathrm{Fr}_\ell^{-2}\right) z_{Sp^n}.$$

However, since $P_\ell(t) \equiv \left(1 - \frac{a_\ell}{\ell}t + \frac{1}{\ell}t^2\right) \mod \ell - 1$, Lemma 9.6.1 of [36] shows that the existence of an Euler system in our sense is equivalent to the existence of an Euler system in the usual sense. Although in this chapter, we show results for Euler systems in our sense, we may replace $P_\ell(t)$ by $\left(1 - \frac{a_\ell}{\ell}t + \frac{1}{\ell}t^2\right)$ in the proofs.

We use the following in order to construct our Euler system from original Kato's Euler system (Theorem 5.2.6).

Proposition 4.2.8. *For every prime $\ell \in \mathscr{R}$, we fix a polynomial $P'_\ell(t) \in \mathbb{Z}_p[t]$ such that*

$$P_\ell(t) \equiv P'_\ell(t) \mod \ell - 1.$$

We suppose that there exists a system $\{z'_{Sp^n}\}_{S\in\mathscr{N},n\geq 0} \in \prod_{S,n} H^1(\mathbb{Q}(Sp^n), T)$ with the following conditions:

1. *For $S \in \mathscr{N}$, a prime $\ell \in \mathscr{R}$ with $\ell \nmid S$ and $n \geq 0$, we have*

$$\mathrm{Cor}_{S\ell/S} z'_{S\ell p^n} = P'_\ell(\mathrm{Fr}_\ell^{-1}) z'_{Sp^n}.$$

2. *For $S \in \mathscr{N}$, the system $\{z'_{Sp^n}\}_{n\geq 0}$ is a norm compatible system.*

Then, there exists an Euler system $\{z_{Sp^n}\}_{S,n}$ in the sense of Definition 4.2.6 such that

(a) for $n \geq 0$ $z_{p^n} = z'_{p^n}$,

(b) for $S \in \mathscr{N}$, $n \geq 0$ and every character χ of Γ_{Sp^n} of conductor Sp^n, we have

$$\sum_{\gamma\in\Gamma_{Sp^n}} \chi(\gamma) z_{Sp^n}^\gamma = \sum_{\gamma\in\Gamma_{Sp^n}} \chi(\gamma)(z'_{Sp^n})^\gamma.$$

Proof. We follow the proof of [36, Lemma 9.6.1]. For a prime $\ell \in \mathscr{R}$, we fix a lift $\mathrm{Fr}_\ell \in G_\mathbb{Q}$ of the arithmetic Frobenius at ℓ, and put

$$d_\ell = P_\ell(\mathrm{Fr}_\ell^{-1}) - P'_\ell(\mathrm{Fr}_\ell^{-1}) \in (\ell - 1)\mathbb{Z}_p[G_\mathbb{Q}].$$

For $S \in \mathscr{N}$ and $n \geq 0$, we put

$$z_{Sp^n} = \sum_{S'|S} \frac{\prod_{\ell'|\frac{S}{S'}} d_{\ell'}}{[\mathbb{Q}(S) : \mathbb{Q}(S')]} z'_{S'p^n},$$

where S' ranges over all positive integers dividing S, and ℓ' ranges over all primes dividing S/S'. For a prime $\ell \in \mathscr{R}$ with $\ell \nmid S$, we have

$$\begin{aligned} z_{S\ell p^n} &= \sum_{S'|S\ell} \frac{\prod_{\ell'|\frac{S\ell}{S'}} d_{\ell'}}{[\mathbb{Q}(S\ell):\mathbb{Q}(S')]} z'_{S'p^n} \\ &= \sum_{S'|S} \frac{\prod_{\ell'|\frac{S}{S'}} d_{\ell'}}{[\mathbb{Q}(S):\mathbb{Q}(S')]} z'_{S'\ell p^n} + \sum_{S'|S} \frac{\prod_{\ell'|\frac{S\ell}{S'}} d_{\ell'}}{[\mathbb{Q}(S\ell):\mathbb{Q}(S')]} z'_{S'p^n} \\ &= \sum_{S'|S} \frac{\prod_{\ell'|\frac{S}{S'}} d_{\ell'}}{[\mathbb{Q}(S):\mathbb{Q}(S')]} z'_{S'\ell p^n} + \frac{d_\ell}{[\mathbb{Q}(\ell):\mathbb{Q}]} \sum_{S'|S} \frac{\prod_{\ell'|\frac{S}{S'}} d_{\ell'}}{[\mathbb{Q}(S):\mathbb{Q}(S')]} z'_{S'p^n}. \end{aligned}$$

From this, we have

$$\begin{aligned} &\mathrm{Cor}_{S\ell p^n/Sp^n} z_{S\ell p^n} \\ =&\mathrm{Cor}_{S\ell p^n/Sp^n} \left(\sum_{S'|S} \frac{\prod_{\ell'|\frac{S}{S'}} d_{\ell'}}{[\mathbb{Q}(S):\mathbb{Q}(S')]} z'_{S'\ell p^n} \right) \\ &\quad + \mathrm{Cor}_{S\ell p^n/Sp^n} \left(\frac{d_\ell}{[\mathbb{Q}(\ell):\mathbb{Q}]} \sum_{S'|S} \frac{\prod_{\ell'|\frac{S}{S'}} d_{\ell'}}{[\mathbb{Q}(S):\mathbb{Q}(S')]} z'_{S'p^n} \right) \\ =&\sum_{S'|S} \frac{\prod_{\ell'|\frac{S}{S'}} d_{\ell'}}{[\mathbb{Q}(S):\mathbb{Q}(S')]} P'_\ell(\mathrm{Fr}_\ell^{-1}) z'_{S'p^n} + d_\ell \sum_{S'|S} \frac{\prod_{\ell'|\frac{S}{S'}} d_{\ell'}}{[\mathbb{Q}(S):\mathbb{Q}(S')]} z'_{S'p^n} \\ =&(P'_\ell(\mathrm{Fr}_\ell^{-1}) + d_\ell) \sum_{S'|S} \frac{\prod_{\ell'|\frac{S}{S'}} d_{\ell'}}{[\mathbb{Q}(S):\mathbb{Q}(S')]} z'_{S'p^n} \\ =&P_\ell(\mathrm{Fr}_\ell^{-1}) z_{Sp^n}. \end{aligned}$$

Since the system $\{z'_{Sp^n}\}_n$ is norm compatible, by the definition of $\{z_{Sp^n}\}_{S,n}$, it is obvious that $\{z_{Sp^n}\}_{n\geq 0}$ is also norm compatible. Thus, we show that $\{z_{Sp^n}\}_{S,n}$ is an Euler system.

The assertion (a) immediately follows from the definition of $\{z_{Sp^n}\}_{S,n}$. We show the assertion (b). Since the conductor of χ is equal to Sp^n, for a proper divisor S' of Sp^n, we have

$$\sum_{\gamma \in \Gamma_{Sp^n}} \chi(\gamma)(z'_{S'})^\gamma = 0.$$

Hence, by the definition of z_{Sp^n}, we deduce the assertion (b). □

Proposition 4.2.9. *Let $\{z_{Sp^n}\}$ be an Euler system and $\lambda \nmid p$ a prime of $\overline{\mathbb{Q}}$. Then, for $S \in \mathscr{N}, n \geq 0$, the image $\mathrm{loc}_\lambda(z_{Sp^n})$ of z_{Sp^n} in $H^1(\mathbb{Q}(Sp^n)_\lambda, T)$ is unramified, that is,*

$$\mathrm{loc}_\lambda(z_{Sp^n}) \in H^1_{\mathrm{ur}}(\mathbb{Q}(Sp^n)_\lambda, T),$$

where $\mathbb{Q}(Sp^n)_\lambda$ denotes the completion at the prime of $\mathbb{Q}(Sp^n)$ below λ.

PROOF. This is a special case of [36, Corollary B.3.5]. We put $K = \mathbb{Q}(S)_\lambda$ and $K_n = \mathbb{Q}(Sp^n)_\lambda$ for $n \geq 1$. We note that K_n/K is unramified, and hence $K_n \subseteq K^{\mathrm{ur}}$. Then, we have an exact sequence

$$0 \to H^1_{\mathrm{ur}}(K_n, T) \to H^1(K_n, T) \to H^0\left(K^{\mathrm{ur}}/K_n, H^1(K^{\mathrm{ur}}, T)\right).$$

By the projective limit with respect to the corestriction maps $H^1(K_{n+1}, T) \to H^1(K_n, T)$, we kave an exact sequence

$$0 \to \varprojlim H^1_{\mathrm{ur}}(K_n, T) \to \varprojlim H^1(K_n, T) \to \varprojlim H^0\left(K^{\mathrm{ur}}/K_n, H^1(K^{\mathrm{ur}}, T)\right).$$

Since $\{\mathrm{loc}_\lambda(z_{Sp^n})\}_n \in \varprojlim H^1(K_n, T)$, we are reduced to showing that

$$\varprojlim H^0\left(K^{\mathrm{ur}}/K_n, H^1(K^{\mathrm{ur}}, T)\right) = 0. \tag{4.2.4}$$

We recall that

$$\begin{aligned} H^0\left(K^{\mathrm{ur}}/K_n, H^1(K^{\mathrm{ur}}, T)\right) &\cong H^1\left(K^{\mathrm{ur}}/K_n, H^1(K^{\mathrm{ur}}, T)^\vee\right)^\vee \\ &\cong H^1\left(K^{\mathrm{ur}}/K_n, H^0(K^{\mathrm{ur}}, E[p^\infty])\right)^\vee, \end{aligned}$$

where $\vee$ denotes the Pontryagin dual $\mathrm{Hom}(-, \mathbb{Q}_p/\mathbb{Z}_p)$. Since $\mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \prod_{\ell:\mathrm{primes}} \mathbb{Z}_\ell$, the field $K_\infty := \cup_n K_n$ is the unique $\mathbb{Z}_p$-extension of K inside K^{ur}. Therefore, we obtain

$$\begin{aligned} \varprojlim H^0\left(K^{\mathrm{ur}}/K_n, H^1(K^{\mathrm{ur}}, T)\right) &\cong \left(\varinjlim H^1\left(K^{\mathrm{ur}}/K_n, H^0(K^{\mathrm{ur}}, E[p^\infty])\right)\right)^\vee \\ &\cong H^1\left(K^{\mathrm{ur}}/K_\infty, H^0(K^{\mathrm{ur}}, E[p^\infty])\right)^\vee. \end{aligned}$$

Since the pro-p-part of $\mathrm{Gal}(K^{\mathrm{ur}}/K_\infty)$ is trivial, its cohomological p-dimension is zero (cf. [32, Corollary 3.3.7]). Hence, we have $H^1\left(K^{\mathrm{ur}}/K_\infty, H^0(K^{\mathrm{ur}}, E[p^\infty])\right)^\vee = 0$, and complete the proof. □

4.2.3 Unramifiedness of derivatives at primes not dividing conductors

For a prime ℓ, we put $m_\ell = [E(\mathbb{Q}_\ell) : E_0(\mathbb{Q}_\ell)]$. We assume that

$$p \nmid 6N \prod_{\ell | N} m_\ell.$$

Let q be a power of p and $\{z_{Sp^n}\}$ an Euler system. For an element $x \in H^1(\mathbb{Q}(S), E[q])$ and a prime λ of $\mathbb{Q}(S)$, we denote by $\mathrm{loc}_\lambda(x)$ the image of x in $H^1(\mathbb{Q}(S)_\lambda, E[q])$.

Proposition 4.2.10. *We suppose that D is a Darmon-Kolyvagin derivative with support S, and put $S' = \mathrm{Cond}(D)$. We assume that $Dz_S \in H^0(\Gamma_S, H^1(\mathbb{Q}(S), T)/q)$ and denote by $\kappa \in H^1(\mathbb{Q}, E[q])$ the inverse image of $Dz_S \in H^1(\mathbb{Q}(S), E[q])$ under the isomorphism (cf. Proposition 4.2.1) $H^1(\mathbb{Q}, E[q]) \cong H^0(\Gamma_S, H^1(\mathbb{Q}(S), E[q]))$. Then, the element κ is unramified outside pS', that is, for every prime $\ell \nmid pS'$ we have*

$$\mathrm{loc}_\ell(\kappa) \in H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, E[q]).$$

Proof. First, we suppose that $\ell \nmid pS$. Since the extension $\mathbb{Q}(S)/\mathbb{Q}$ is unramified at ℓ, we have $(\mathbb{Q}(S)_\lambda)^{\mathrm{ur}} \cong \mathbb{Q}_\ell^{\mathrm{ur}}$ for a prime $\lambda|\ell$. Hence, we have $\mathrm{loc}_\ell(\kappa) = \mathrm{loc}_\lambda(Dz_S)$ as elements of $H^1(\mathbb{Q}_\ell^{\mathrm{ur}}, E[q])$. By Proposition 4.2.9, we have $\mathrm{loc}_\ell(\kappa) \in H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, E[q])$.

We next consider a prime ℓ dividing S/S'. Then we have

$$Dz_S = D'N_\ell z_S = P_\ell(\mathrm{Fr}_\ell^{-1})D'z_{S/\ell},$$

where D' is a derivative such that $\mathrm{Supp}(D') = S/\ell$. Since the extension $\mathbb{Q}(S/\ell)/\mathbb{Q}$ is unramified at ℓ, for a prime λ of $\mathbb{Q}(S/\ell)$ we have $\mathrm{loc}_\ell(\kappa) = \mathrm{loc}_\lambda(D'P_\ell(\mathrm{Fr}_\ell^{-1})z_{S/\ell})$ as elements of $H^1(\mathbb{Q}_\ell^{\mathrm{ur}}, E[q])$. Then by Proposition 4.2.9, we complete the proof. □

Corollary 4.2.11. *Under the notation as above, for every prime $\ell \nmid pS'$, we have*

$$\mathrm{loc}_\ell(\kappa) \in E(\mathbb{Q}_\ell)/q.$$

Proof. The proof is based on that of [8, Theorem 4.9]. By the exact sequence

$$0 \to E(\mathbb{Q}_\ell)/q \to H^1(\mathbb{Q}_\ell, E[q]) \to H^1(\mathbb{Q}_\ell, E)[q] \to 0,$$

it suffices to show that the image of κ in $H^1(\mathbb{Q}_\ell, E)[q]$ is trivial. Proposition 4.2.10 shows that the image of κ in $H^1(\mathbb{Q}_\ell, E)[q]$ comes from $H^1(\mathbb{Q}_\ell^{\mathrm{ur}}/\mathbb{Q}_\ell, E(\mathbb{Q}_\ell^{\mathrm{ur}}))[q]$. By Proposition 2.1.3, we have

$$H^1(\mathbb{Q}_\ell^{\mathrm{ur}}/\mathbb{Q}_\ell, E(\mathbb{Q}_\ell^{\mathrm{ur}}))[q] = H^1\left(\mathbb{Q}_\ell^{\mathrm{ur}}/\mathbb{Q}_\ell, \pi_0\left(\mathscr{E}_{\overline{\mathbb{F}}_\ell}\right)\right)[q],$$

where $\mathscr{E}$ denotes the Néron model of E over $\mathrm{Spec}(\mathbb{Z}_\ell^{\mathrm{ur}})$, and $\pi_0\left(\mathscr{E}_{\overline{\mathbb{F}}_\ell}\right)$ denotes the group of connected components of the special fiber $\mathscr{E}_{\overline{\mathbb{F}}_\ell}$. Since $p \nmid m_\ell$ (if $\ell \nmid N$, then $\pi_0\left(\mathscr{E}_{\overline{\mathbb{F}}_\ell}\right)$ is trivial), we have

$$H^1\left(\mathbb{Q}_\ell^{\mathrm{ur}}/\mathbb{Q}_\ell, \pi_0\left(\mathscr{E}_{\overline{\mathbb{F}}_\ell}\right)\right)[q] = 0,$$

and hence conclude that the image of κ in $H^1(\mathbb{Q}_\ell, E)[q]$ is trivial.

□

4.2.4 Local behavior at primes dividing conductors

As in the previous subsection, let q be a power of p. We put

$$\begin{aligned} \mathscr{R}_q &= \{\ell \in \mathscr{R} \ ; \ q|\ell - 1\}, \\ \mathscr{R}_{E,q} &= \{\ell \in \mathscr{R}_q \ ; \ q|P_\ell(1)\}, \\ \mathscr{N}_q &= \{\text{square-free products of primes in } \mathscr{R}_q\}. \end{aligned} \tag{4.2.5}$$

We take an element $S \in \mathscr{N}_p$. The aim of this subsection is to compare Dz_S with $DD_\ell^{(1)} z_{S\ell}$ under the localization at primes dividing ℓ. See Theorem 4.2.21 for the precise statement.

Definition 4.2.12. Let $n \geq 0$. For a positive divisor S' of S, let $x_{S'p^n}$ denote an indeterminate. We denote by Y_{Sp^n} the free $\mathbb{Z}_p[\Gamma_{Sp^n}]$-module generated by $\{x_{S'p^n}\}_{S'|S>0}$, that is, $Y_{Sp^n} = \oplus_{S'|S>0}\mathbb{Z}_p[\Gamma_{Sp^n}]x_{S'p^n}$. We denote by Z_{Sp^n} the submodule of Y_{Sp^n} generated by

$$\sigma x_{S'p^n} - x_{S'p^n} \text{ for } S'|S, \sigma \in \Gamma_{S/S'} \text{ and } \quad N_\ell x_{S'\ell p^n} - P_\ell(\mathrm{Fr}_\ell^{-1}) x_{S'p^n} \text{ for primes } \ell \text{ with } \ell S'|S.$$

We define $X_{Sp^n} = Y_{Sp^n}/Z_{Sp^n}$.

If we regard $z_{S'p^n}$ as an element of $H^1(\mathbb{Q}(Sp^n), T)$ for $S'|S$ by the restriction map, then there exists a unique homomorphism of Γ_{Sp^n}-modules

$$g_{Sp^n} : X_{Sp^n} \to H^1(\mathbb{Q}(Sp^n), T)$$

sending $x_{S'p^n}$ to $z_{S'p^n}$ for $S'|S$.

Lemma 4.2.13. *For a square-free integer m, we have*

$$\sum_{d|m,\ d>1} \prod_{\ell|d:\text{primes}} (|\Gamma_\ell| - 1) = |\Gamma_m| - 1.$$

Proof. We prove the lemma by induction on the number of primes dividing m. If m is a prime, then there is nothing to prove.

In the general case, we write $m = \ell_0 m'$, where ℓ_0 is a prime. Then we have

$$\begin{aligned} \sum_{d|m,\ d>1} \prod_{\ell|d:\text{primes}} (|\Gamma_\ell| - 1) &= \sum_{d|m',\ d>1} \prod_{\ell|d} (|\Gamma_\ell| - 1) + \sum_{d|m,\ \ell_0|d} \prod_{\ell|d} (|\Gamma_\ell| - 1) \\ &= |\Gamma_{m'}| - 1 + (|\Gamma_{\ell_0}| - 1) \left\{ \sum_{d'|m',\ d'>1} \prod_{\ell|d'} (|\Gamma_\ell| - 1) + 1 \right\} \\ &= |\Gamma_{m'}| - 1 + (|\Gamma_{\ell_0}| - 1)|\Gamma_{m'}| \\ &= |\Gamma_{m'}||\Gamma_{\ell_0}| - 1 \\ &= |\Gamma_m| - 1, \end{aligned}$$

where the second and the third equalities follow from the induction hypothesis. □

We review properties of X_{Sp^n}.

Proposition 4.2.14. *1. The $\mathbb{Z}_p[\Gamma_{Sp^n}]$-module X_{Sp^n} is a free $\mathbb{Z}_p$-module of finite rank.*

2. The $\mathbb{Q}_p[\Gamma_{Sp^n}]$-module $X_{Sp^n} \otimes \mathbb{Q}_p$ is free of rank 1.

Proof. We follow the proof of [36, Proposition 4.3.1]. For each prime ℓ dividing S, we put $A_\ell = \Gamma_\ell \setminus \{1\} \subset \Gamma_{Sp^n}$. Since $S \in \mathscr{N}_p$, we have $A_\ell \neq \emptyset$. For a positive integer S' dividing S, we define a subset $A_{n,S'} \subset \Gamma_{S'p^n}$ by

$$A_{n,S'} = \Gamma_{p^n} \prod_{\ell|S':\text{prime}} A_\ell = \left\{ g_n \prod_{\ell|S'} \gamma_\ell \ ; \ g_n \in \Gamma_{p^n},\ 1 \neq \gamma_\ell \in \Gamma_\ell \right\} \qquad \text{if } S' > 1,$$

$$A_{n,S'} = \Gamma_{p^n} \qquad \text{if } S' = 1.$$

We define a finite subset B_{Sp^n} of X_{Sp^n} by

$$B_{Sp^n} = \bigcup_{S'|S} A_{n,S'} x_{S'p^n} \subset X_{Sp^n},$$

where $A_{n,S'} x_{S'p^n} := \{g x_{S'p^n};\ g \in A_{n,S'}\}$. Our goal is to show that B_{Sp^n} is a $\mathbb{Z}_p$-basis of X_{Sp^n}.

Claim 1. For $S'|S$, the finite set $\Gamma_{p^n} \prod_{\ell|S'}(A_\ell \cup \{N_\ell\})$ generates $\mathbb{Z}_p[\Gamma_{S'p^n}]$ over $\mathbb{Z}_p$.

Proof of Claim 1. In the case where S' is a prime ℓ, we note that $1 = N_\ell - \sum_{\gamma_\ell \in A_\ell} \gamma_\ell$ in $\mathbb{Z}_p[\Gamma_\ell]$, and then the finite set $A_\ell \cup \{N_\ell\}$ generates $\mathbb{Z}_p[\Gamma_\ell]$ over $\mathbb{Z}_p$. Hence, the finite set $\Gamma_{p^n} \prod_{\ell|S'}(A_\ell \cup \{N_\ell\})$ generates $\mathbb{Z}_p[\Gamma_{\ell p^n}]$ over $\mathbb{Z}_p$. In the general case, we have

$$1 = \prod_{\ell|S'} \left(N_\ell - \sum_{\gamma_\ell \in A_\ell} \gamma_\ell \right) \quad \text{in } \mathbb{Z}_p[\Gamma_{S'}].$$

We note that this product belongs to the $\mathbb{Z}_p$-submodule generated by $\prod_{\ell|S'}(A_\ell \cup \{N_\ell\})$. Hence the finite set $\Gamma_{p^n} \prod_{\ell|S'}(A_\ell \cup \{N_\ell\})$ generates $\mathbb{Z}_p[\Gamma_{S'p^n}]$ over $\mathbb{Z}_p$ for $S'|S$.

Claim 2. The finite set B_{Sp^n} generates X_{Sp^n} over $\mathbb{Z}_p$.

Proof of Claim 2. We prove the claim by induction on the number of primes dividing S. For a subset B of X_{Sp^n}, we denote by $\mathbb{Z}_p[B]$ the $\mathbb{Z}_p$-submodule of X_{Sp^n} by B.

In the case $S = \ell$ is a prime, it is clear that $\mathbb{Z}_p[\Gamma_{p^n}]x_{p^n} \subseteq \mathbb{Z}_p[B_{\ell p^n}]$. Then it suffices to show that $\mathbb{Z}_p[\Gamma_{\ell p^n}]x_{\ell p^n} \subseteq \mathbb{Z}_p[B_{\ell p^n}]$. Since $N_\ell x_{\ell p^n} = P_\ell(\mathrm{Fr}_\ell^{-1}) x_{p^n}$, we have

$$N_\ell x_{\ell p^n} \in \mathbb{Z}_p[B_{p^n}] \subseteq \mathbb{Z}_p[B_{\ell p^n}]. \tag{4.2.6}$$

By definition,

$$\gamma_\ell x_{\ell p^n} \in \mathbb{Z}[B_{\ell p^n}] \text{ for } \gamma_\ell \in A_\ell. \tag{4.2.7}$$

Combining (4.2.6) and (4.2.7), we have

$$(A_\ell \cup \{N_\ell\}) x_{\ell p^n} \in \mathbb{Z}_p[B_{\ell p^n}].$$

Hence, by Claim 1, obtain

$$\mathbb{Z}_p[\Gamma_{\ell p^n}] x_{\ell p^n} \subseteq \mathbb{Z}_p[B_{\ell p^n}].$$

In the general case, we write $S = \ell_1 \cdots \ell_s$. For a proper divisor S' of S, by the induction hypothesis, we have

$$\mathbb{Z}_p[\Gamma_{Sp^n}] x_{S'p^n} = \mathbb{Z}_p[\Gamma_{S'p^n}] x_{S'p^n} \subseteq \mathbb{Z}_p[B_{S'p^n}] \subseteq \mathbb{Z}_p[B_{Sp^n}].$$

Therefore, by Claim 1, we are reduced to showing that

$$\left(\prod_{\ell | S} (A_\ell \cup \{N_\ell\}) \right) x_{Sp^n} \subset \mathbb{Z}_p[B_{Sp^n}].$$

We take an element $\gamma \in \prod_{\ell|S}(A_\ell \cup \{N_\ell\})$. Then, we have $\gamma = \left(\prod_{\ell'|S_1} \gamma_{\ell'}\right) \cdot N_{S_2}$, where $S = S_1 S_2$, $\gamma_{\ell'} \in A_{\ell'}$ for $\ell' | S_1$. When $S = S_1$, we have $\gamma x_{Sp^n} \in \mathbb{Z}_p[B_{Sp^n}]$ by definition. Hence, we assume that $S \neq S_1$. Then, we have

$$\gamma x_{Sp^n} = \left(\prod_{\ell' | S_1} \gamma_{\ell'} \right) N_{S_2} x_{Sp^n} = \left(\prod_{\ell' | S_1} \gamma_{\ell'} \right) \left(\prod_{\ell | S_2} P_\ell(\mathrm{Fr}_\ell^{-1}) \right) x_{S_1 p^n}.$$

By the induction hypothesis, we obtain $\left(\prod_{\ell'|S_1} \gamma_{\ell'}\right) \left(\prod_{\ell|S_2} P_\ell(\mathrm{Fr}_\ell^{-1})\right) x_{S_1 p^n} \in \mathbb{Z}_p[B_{S_1 p^n}]$, and hence $\gamma x_{Sp^n} \in \mathbb{Z}_p[B_{Sp^n}]$. Thus, we complete the proof of the claim.

We define a $\mathbb{Q}_p[\Gamma_{Sp^n}]$-morphism φ from $X_{Sp^n} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ to $\mathbb{Q}_p[\Gamma_{Sp^n}]$ by

$$\varphi(x_{S'p^n}) = \prod_{\ell' | (S/S') : \text{primes}} N_{\ell'} \prod_{\ell | S' : \text{primes}} \left(|\Gamma_\ell| + (P_\ell(\mathrm{Fr}_\ell^{-1}) - |\Gamma_\ell|) \frac{N_\ell}{|\Gamma_\ell|} \right) \quad \text{for } S' | S.$$

Claim 3. The map φ is well-defined and surjective.

Proof of Claim 3. For the well-definedness, we show that $\varphi(Z_{Sp^n}) = 0$ for Z_{Sp^n} as in Definition 4.2.12. Let $S'|S$ and $\sigma \in \Gamma_{S/S'}$. Then, we have

$$\begin{aligned} \varphi(\sigma x_{S'p^n} - x_{S'p^n}) &= (\sigma - 1)\varphi(x_{S'p^n}) \\ &= (\sigma - 1) \prod_{\ell' | (S/S')} N_{\ell'} \prod_{\ell | S'} \left(|\Gamma_\ell| + (P_\ell(\mathrm{Fr}_\ell^{-1}) - |\Gamma_\ell|) \frac{N_\ell}{|\Gamma_\ell|} \right) \end{aligned}$$

$$= 0,$$

where the last equality follows from $(\sigma - 1)\prod_{\ell'|(S/S')} N_{\ell'} = (\sigma - 1)\sum_{\gamma' \in \Gamma_{S/S'}} \gamma = 0$. We next pick a prime ℓ_0 dividing S/S'. We have

$$\varphi(N_{\ell_0} x_{S'\ell_0 p^n} - P_{\ell_0}(\mathrm{Fr}_{\ell_0}^{-1}) x_{S'p^n}) = N_{\ell_0}\varphi(x_{S'\ell_0 p^n}) - P_{\ell_0}(\mathrm{Fr}_{\ell_0}^{-1})\varphi(x_{S'p^n}).$$

By using $N_{\ell_0} N_{\ell_0} = |\Gamma_{\ell_0}| N_{\ell_0}$, we obtain

$$\begin{aligned}
&N_{\ell_0}\varphi(x_{S'\ell_0 p^n}) \\
=&N_{\ell_0} \prod_{\ell' | \frac{S}{S'\ell_0}} N_{\ell'} \prod_{\ell | S'\ell_0} \left(|\Gamma_\ell| + (P_\ell(\mathrm{Fr}_\ell^{-1}) - |\Gamma_\ell|)\frac{N_\ell}{|\Gamma_\ell|} \right) \\
=&\left(|\Gamma_{\ell_0}| + (P_{\ell_0}(\mathrm{Fr}_{\ell_0}^{-1}) - |\Gamma_{\ell_0}|)\frac{N_{\ell_0}}{|\Gamma_{\ell_0}|} \right) N_{\ell_0} \prod_{\ell' | \frac{S}{S'\ell_0}} N_{\ell'} \prod_{\ell | S'} \left(|\Gamma_\ell| + (P_\ell(\mathrm{Fr}_\ell^{-1}) - |\Gamma_\ell|)\frac{N_\ell}{|\Gamma_\ell|} \right) \\
=&\left(|\Gamma_{\ell_0}| + (P_{\ell_0}(\mathrm{Fr}_{\ell_0}^{-1}) - |\Gamma_{\ell_0}|)\frac{|\Gamma_{\ell_0}|}{|\Gamma_{\ell_0}|} \right) N_{\ell_0} \prod_{\ell' | \frac{S}{S'\ell_0}} N_{\ell'} \prod_{\ell | S'} \left(|\Gamma_\ell| + (P_\ell(\mathrm{Fr}_\ell^{-1}) - |\Gamma_\ell|)\frac{N_\ell}{|\Gamma_\ell|} \right) \\
=&P_{\ell_0}(\mathrm{Fr}_{\ell_0}^{-1}) \prod_{\ell' | \frac{S}{S'}} N_{\ell'} \prod_{\ell | S'} \left(|\Gamma_\ell| + (P_\ell(\mathrm{Fr}_\ell^{-1}) - |\Gamma_\ell|)\frac{N_\ell}{|\Gamma_\ell|} \right) \\
=&P_{\ell_0}(\mathrm{Fr}_{\ell_0}^{-1})\varphi(x_{S'p^n}).
\end{aligned}$$

Hence,

$$\varphi(N_{\ell_0} x_{S'\ell_0 p^n} - P_{\ell_0}(\mathrm{Fr}_{\ell_0}^{-1}) x_{S'p^n}) = 0.$$

Then, we deduce that φ is well-defined. We next show that φ is surjective. We recall that $\mathbb{Q}_p[\Gamma_{Sp^n}] \cong \prod_\chi K_\chi$, where χ ranges over all the characters of Γ_{Sp^n} and $K_\chi := \mathbb{Q}_p[\mathrm{Im}(\chi)]$. For each character χ of Γ_{Sp^n} of conductor $S'p^m$, we have

$$\begin{aligned}
\chi(\varphi(x_{S'p^n})) &= \prod_{\ell' | (S/S')} \chi(N_{\ell'}) \prod_{\ell | S'} \left(|\Gamma_\ell| + (P_\ell(\chi(\mathrm{Fr}_\ell^{-1})) - |\Gamma_\ell|)\frac{\chi(N_\ell)}{|\Gamma_\ell|} \right) \\
&= \prod_{\ell' | (S/S')} |\Gamma_{\ell'}| \prod_{\ell | S'} |\Gamma_\ell| = \prod_{\ell | S} |\Gamma_\ell| \neq 0.
\end{aligned}$$

This shows that $\mathrm{Im}(\varphi)$ is an ideal of $\mathbb{Q}_p[\Gamma_{Sp^n}]$ not contained in any maximal ideal of $\mathbb{Q}_p[\Gamma_{Sp^n}]$ and hence is equal to $\mathbb{Q}[\Gamma_{Sp^n}]$. Thus, we deduce that φ is surjective, and conclude the claim.

By definition, we have

$$|B_{Sp^n}| \leq \sum_{S'|S} |A_{n,S'}| = \sum_{S'|S,\ S'>1} |\Gamma_{p^n}| \prod_{\ell | S'} |A_\ell| + |\Gamma_{p^n}|$$

$$= |\Gamma_{p^n}| \left(\sum_{S' | S,\ S' > 1} \prod_{\ell | S'} (|\Gamma_\ell| - 1) + 1 \right)$$
$$= |\Gamma_{Sp^n}| \quad \text{by Lemma 4.2.13.}$$

Then, Claim 3 shows that

$$\mathrm{rank}_{\mathbb{Z}_p}(X_{Sp^n}) = \dim_{\mathbb{Q}_p}(X_{Sp^n} \otimes \mathbb{Q}_p) \geq |\Gamma_{Sp^n}| \geq |B_{Sp^n}|.$$

By Claim 2, we have $\mathrm{rank}_{\mathbb{Z}_p}(X_{Sp^n}) \leq |B_{Sp^n}|$ and deduce the assertion 1 of the proposition. We also have

$$\mathrm{rank}_{\mathbb{Z}_p}(X_{Sp^n}) = \dim_{\mathbb{Q}_p}(X_{Sp^n} \otimes \mathbb{Q}_p) = |\Gamma_{Sp^n}| = |B_{Sp^n}|,$$

and hence by Claim 3, the map φ is an isomorphism. Thus, we complete the proof. □

Lemma 4.2.15. *Let R be a ring and G a finite abelian group. Suppose that B is an $R[G]$-module. Then, the following assertions hold.*

1. $\mathrm{Hom}_{R[G]}(B, R[G]) \cong \mathrm{Hom}_R(B, R)$ *as R-modules.*
2. *If B is free as an R-module then* $\mathrm{Ext}^1_{R[G]}(B, R[G]) = 0$.

Proof. We denote by ξ the R-morphism from $R[G]$ to R defined as

$$R[G] \to R;\ \sum_{\sigma \in G} a_\sigma \sigma \mapsto a_1.$$

We define

$$\phi : \mathrm{Hom}_{R[G]}(B, R[G]) \to \mathrm{Hom}_R(B, R) \quad \text{by } \phi(f)(b) = \xi(f(b)) \text{ for } b \in B.$$

We show that the inverse ψ of ϕ is given by

$$\psi : \mathrm{Hom}_R(B, R) \to \mathrm{Hom}_{R[G]}(B, R[G]);\ h \mapsto \left(b \mapsto \sum_{\sigma \in G} h(\sigma^{-1} b)\sigma \right).$$

To show that $\psi \circ \phi = \mathrm{id}$, we take an element $f \in \mathrm{Hom}_{R[G]}(B, R[G])$. For an element $b \in B$, we write $f(b) = \sum_{g \in G} a_g g$, and then have

$$(\psi \circ \phi(f))(b) = \sum_{\sigma \in G} \left(\phi(f)(\sigma^{-1} b) \right) \sigma = \sum_{\sigma \in G} \xi \left(\sigma^{-1} \sum_{g \in G} a_g g \right) \sigma$$
$$= \sum_{\sigma \in G} \xi \left(\sum_{g \in G} a_{\sigma g} g \right) \sigma = \sum_{\sigma \in G} a_\sigma \sigma = f(b),$$

which implies that $\psi \circ \phi = \mathrm{id}$. Next, we prove that $\phi \circ \psi = \mathrm{id}$. We take elements $h \in \mathrm{Hom}_R(B, R)$, $b \in B$. Then,

$$\phi \circ \psi(f)(b) = \xi\left(\psi(f)(b)\right) = \xi\left(\sum_{\sigma \in G} h(\sigma^{-1}b)\sigma\right) = h(b).$$

From this we have $\psi \circ \phi = \mathrm{id}$, and hence $\mathrm{Hom}_{R[G]}(B, R[G]) \cong \mathrm{Hom}_R(B, R)$. Furthermore, we have

$$\mathrm{Ext}^1_{R[G]}(B, R[G]) \cong \mathrm{Ext}^1_R(B, R),$$

which is zero when B is R-free. □

Corollary 4.2.16. *For $k \geq 0$, we have*

$$\mathrm{Ext}^1_{\mathbb{Z}/q\mathbb{Z}[\Gamma_{Sp^n}]}(X_{Sp^n}/qX_{Sp^n}, \mathbb{Z}/q\mathbb{Z}[\Gamma_{Sp^n}]^{\oplus k}) = 0.$$

Proof. We apply Lemma 4.2.15 with

$$R = \mathbb{Z}/q\mathbb{Z}, \quad G = \Gamma_{Sp^n}, \quad H = \{1\}, \quad B = X_{Sp^n}/qX_{Sp^n}.$$

Then the corollary follows from the assertion 1 of Proposition 4.2.14. □

We put $M_q = \mathrm{Ind}_{\{1\}}^{G_{\mathbb{Q}}}(E[q])$. We recall that $\mathrm{Ind}_{\{1\}}^{G_{\mathbb{Q}}}(E[q])$ is defined as the module of continuous maps from $G_{\mathbb{Q}}$ to $E[q]$, and $G_{\mathbb{Q}}$ acts on $\mathrm{Ind}_{\{1\}}^{G_{\mathbb{Q}}}(E[q])$ by $(\sigma f)(g) = f(g\sigma)$ for $\sigma, g \in G_{\mathbb{Q}}$. Then we have an exact sequence of $G_{\mathbb{Q}}$-modules

$$0 \to E[q] \to M_q \to M_q/E[q] \to 0,$$

where the map $E[q] \to M_q$ is defined as $y \mapsto (g \mapsto gy)$. For a finite extension L of $\mathbb{Q}$, by taking Galois cohomology, we obtain an exact sequence

$$0 \to E(L)[q] \to M_q^{G_L} \to (M_q/E[q])^{G_L} \xrightarrow{\delta_L} H^1(L, E[q]) \to 0. \tag{4.2.8}$$

See [36, Proposition B.4.5] for the surjectivity of the connecting map δ_L.

Lemma 4.2.17. *The $\mathbb{Z}/q\mathbb{Z}[\Gamma_{Sp^n}]$-module $M_q^{G_{\mathbb{Q}(Sp^n)}}$ is free of rank two.*

Proof. We have

$$M_q^{G_{\mathbb{Q}(Sp^n)}} = \left(\mathrm{Ind}_{\{1\}}^{G_{\mathbb{Q}}}(E[q])\right)^{G_{\mathbb{Q}(Sp^n)}} = \mathrm{Ind}_{\{1\}}^{\Gamma_{Sp^n}}(E[q]) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}/q\mathbb{Z}[\Gamma_{Sp^n}], E[q]),$$

which is a free $\mathbb{Z}/q\mathbb{Z}[\Gamma_{Sp^n}]$-module of rank two. □

Proposition 4.2.18. *There is a homomorphism d_{Sp^n} of Γ_{Sp^n}-modules from X_{Sp^n} to $(M_q/E[q])^{G_{\mathbb{Q}(Sp^n)}}$ making the following diagram commutative*:

$$\begin{array}{ccc} & & (M_q/E[q])^{G_{\mathbb{Q}(Sp^n)}} \\ & \overset{d_{Sp^n}}{\nearrow} & \Big\downarrow{\scriptstyle \delta_{\mathbb{Q}(Sp^n)}} \\ X_{Sp^n} & \xrightarrow[g_{Sp^n}]{} & H^1(\mathbb{Q}(Sp^n), E[q]). \end{array}$$

Proof. We put $R = \mathbb{Z}/q\mathbb{Z}$. By Proposition 4.2.1, we have $E(\mathbb{Q}(Sp^n))[q] = 0$. Therefore, by (4.2.8), we have an exact sequence

$$0 \to M_q^{G_{\mathbb{Q}(Sp^n)}} \to (M_q/E[q])^{G_{\mathbb{Q}(Sp^n)}} \xrightarrow{\delta_{\mathbb{Q}(Sp^n)}} H^1(\mathbb{Q}(Sp^n), E[q]) \to 0.$$

Then, we have an exact sequence

$$\begin{aligned} 0 \to &\mathrm{Hom}_{R[\Gamma_{Sp^n}]}(X_{Sp^n}/q, M_q^{G_{\mathbb{Q}(Sp^n)}}) \to \mathrm{Hom}_{R[\Gamma_{Sp^n}]}(X_{Sp^n}/q, (M_q/E[q])^{G_{\mathbb{Q}(Sp^n)}}) \\ &\to \mathrm{Hom}_{R[\Gamma_{Sp^n}]}(X_{Sp^n}/q, H^1(\mathbb{Q}(Sp^n), E[q])) \to \mathrm{Ext}^1_{R[\Gamma_{Sp^n}]}(X_{Sp^n}/q, M_q^{G_{\mathbb{Q}(Sp^n)}}). \end{aligned} \tag{4.2.9}$$

By Proposition 4.2.16 and Lemma 4.2.17, we have $\mathrm{Ext}^1_{R[\Gamma_{Sp^n}]}(X_{Sp^n}/q, M_q^{G_{\mathbb{Q}(Sp^n)}}) = 0$. Hence, the map

$$\mathrm{Hom}_{R[\Gamma_{Sp^n}]}(X_{Sp^n}/q, (M_q/E[q])^{G_{\mathbb{Q}(Sp^n)}}) \to \mathrm{Hom}_{R[\Gamma_{Sp^n}]}(X_{Sp^n}/q, H^1(\mathbb{Q}(Sp^n), E[q]))$$

is surjective. We let $d_{Sp^n} \in \mathrm{Hom}_{R[\Gamma_{Sp^n}]}(X_{Sp^n}/q, (M_q/E[q])^{G_{\mathbb{Q}(Sp^n)}})$ be a lift of g_{Sp^n} under the map, and complete the proof. □

We take a prime $\ell \in \mathscr{R}_{E,q}$ which splits completely in $\mathbb{Q}(S)$. We denote by $\mathscr{D}_\ell \subseteq G_\mathbb{Q}$ a decomposition group of ℓ, and by $\mathscr{I}_\ell \subset \mathscr{D}_\ell$ the inertia group. Then, the natural map $\mathscr{I}_\ell \to \Gamma_\ell$ is surjective. We fix a lift of σ_ℓ to $\mathscr{I}_\ell$, which we also denote by σ_ℓ. We recall that for a power m of p, we have an isomorphism of $\mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{ur}}/\mathbb{Q}_\ell)$-modules defined as

$$\mathscr{I}_\ell/\mathscr{I}_\ell^m \to \mu_m;\ \sigma \mapsto \frac{\sigma\ell^{1/m}}{\ell^{1/m}}.$$

From this, the quotient $\mathscr{I}_\ell/\mathscr{I}_\ell^{|\Gamma_\ell|}$ is cyclic, and hence $\mathscr{I}_\ell/\mathscr{I}_\ell^{|\Gamma_\ell|} \cong \Gamma_\ell$. Since Γ_ℓ is generated by σ_ℓ, the quotient $\mathscr{I}_\ell/\mathscr{I}_\ell^{|\Gamma_\ell|}$ is also generated by σ_ℓ. Since $q|\Gamma_\ell$, the quotient $\mathscr{I}_\ell/\mathscr{I}_\ell^q$ is generated by σ_ℓ.

Lemma 4.2.19. *Let d_{Sp^n} be a homomorphism of Γ_{Sp^n}-modules as in Proposition* 4.2.18. *We take a lift $\hat{d}(x_{Sp^n}) \in M_q$ of $d_S(x_{Sp^n})$. Then, for $\gamma \in G_\mathbb{Q}$ and $\rho, \rho' \in \mathscr{D}_\ell$, we have*

$$\rho\rho'\gamma\hat{d}(x_{Sp^n}) = \rho'\rho\gamma\hat{d}(x_{Sp^n}) \quad \textit{in } M_q.$$

PROOF. We follow the proof of [36, Lemma 4.7.1]. Since the extension $\mathbb{Q}(Sp^n)/\mathbb{Q}$ is unramified at ℓ, we have $\mathscr{I}_\ell \subseteq G_{\mathbb{Q}(Sp^n)}$. If we denote by $\mathrm{res}_{\mathscr{I}_\ell}$ the restriction map $H^1(\mathbb{Q}(Sp^n), E[q]) \to H^1(\mathscr{I}_\ell, E[q])$, then Proposition 4.2.9 implies that

$$\mathrm{res}_{\mathscr{I}_\ell}(\gamma z_{Sp^n}) = 0 \quad \text{in } H^1(\mathscr{I}_\ell, E[q]) = \mathrm{Hom}(\mathscr{I}_\ell, E[q]).$$

Since $\delta_{Sp^n}(\gamma x_{Sp^n}) = \gamma z_{Sp^n}$, the definition of the connecting map δ_{Sp^n} shows that for $\sigma \in \mathscr{I}_\ell$,

$$(\sigma - 1)\gamma\hat{d}(x_{Sp^n}) = (\gamma z_{Sp^n})(\sigma) = 0 \quad \text{in } E[q]. \tag{4.2.10}$$

Since $\mathscr{D}_\ell/\mathscr{I}_\ell = \mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{ur}}/\mathbb{Q}_\ell)$ is abelian, we have$(\rho'\rho)^{-1}\rho\rho' \in \mathscr{I}_\ell$. Then, we may apply (4.2.10) with $\sigma = (\rho'\rho)^{-1}\rho\rho'$, and complete the proof. □

We fix a lift $\mathrm{Fr}_\ell \in \mathscr{D}_\ell$ of the arithmetic Frobenius at ℓ. By abuse of notation, we put

$$N_\ell = \sum_{i=1}^{n_\ell} \sigma_\ell^i, \quad D_\ell^{(1)} = \sum_{i=0}^{n_\ell - 1} i\sigma_\ell^i \quad \in \mathbb{Z}[\mathscr{I}_\ell],$$

where $n_\ell := |\Gamma_\ell|$. Then we have

$$(\sigma_\ell - 1)D_\ell^{(1)} = n_\ell \sigma_\ell^{n_\ell} - N_\ell \quad \text{in } \mathbb{Z}[\mathscr{I}_\ell]. \tag{4.2.11}$$

Lemma 4.2.20. *For a homomorphism $d_{S\ell p^n} : X_{S\ell p^n} \to M_q/E[q]$ as in Proposition 4.2.18, we take lifts $\hat{d}(x_{S\ell p^n}), \hat{d}(x_{Sp^n}) \in M_q$ of $d_{S\ell p^n}(x_{S\ell p^n}), d_{S\ell p^n}(x_{Sp^n})$, respectively. Then, for every $\gamma \in G_\mathbb{Q}$, we have*

$$N_\ell\gamma\hat{d}(x_{S\ell p^n}) = P_\ell(\mathrm{Fr}_\ell^{-1})\gamma\hat{d}(x_{Sp^n}) \quad \textit{in } M_q.$$

PROOF. We follow the proof of [36, Lemma 4.7.3]. Since $d_{S\ell p^n}$ is $G_\mathbb{Q}$-equivariant, the equation $N_\ell x_{S\ell p^n} = P_\ell(\mathrm{Fr}_\ell^{-1})x_{Sp^n}$ implies that

$$N_\ell\gamma d_{S\ell p^n}(x_{S\ell p^n}) = P_\ell(\mathrm{Fr}_\ell^{-1})\gamma d_{Sp^n}(x_{Sp^n}),$$

and hence

$$N_\ell\gamma\hat{d}(x_{S\ell p^n}) - P_\ell(\mathrm{Fr}_\ell^{-1})\gamma\hat{d}(x_{Sp^n}) \in E[q].$$

Claim. The element $N_\ell\gamma\hat{d}(x_{S\ell p^n}) - P_\ell(\mathrm{Fr}_\ell^{-1})\gamma\hat{d}(x_{Sp^n})$ of $E[q]$ is independent of the choices of $d_{S\ell p^n}, \hat{d}(x_{S\ell p^n})$ and $\hat{d}(x_{Sp^n})$.

Proof of Claim. We take another choice $d'_{S\ell p^n}$ of $d_{S\ell p^n}$. By the exact sequence (4.2.9), we may write

$$d'_{S\ell p^n} = d_{S\ell p^n} + d_0 \text{ for some } d_0 \in \mathrm{Hom}_{G_\mathbb{Q}}(X_{S\ell p^n}, M_q).$$

If we choose lifts $\hat{d}'(x_{S\ell p^n}),\ \hat{d}'(x_{Sp^n}) \in M_q$ of $d'_{S\ell p^n}(x_{S\ell p^n}),\ d'_{S\ell p^n}(x_{Sp^n}) \in M_q/E[q]$, respectively, then we have

$$\hat{d}'(x_{S\ell p^n}) = \hat{d}(x_{S\ell p^n}) + d_0(x_{S\ell p^n}) + a, \quad \hat{d}'(x_{Sp^n}) = \hat{d}(x_{Sp^n}) + d_0(x_{Sp^n}) + a', \tag{4.2.12}$$

where $a, a' \in E[q]$. Since d_0 is $G_{\mathbb{Q}}$-equivariant, by (4.2.12), we have

$$\begin{aligned}
&N_\ell\gamma\hat{d}'(x_{S\ell p^n}) - P_\ell(\mathrm{Fr}_\ell^{-1})\gamma\hat{d}'(x_{Sp^n}) - \left(N_\ell\gamma\hat{d}(x_{S\ell p^n}) - P_\ell(\mathrm{Fr}_\ell^{-1})\gamma\hat{d}(x_{Sp^n})\right)\\
&= N_\ell\gamma\left(\hat{d}'(x_{S\ell p^n}) - \hat{d}(x_{S\ell p^n})\right) - P_\ell(\mathrm{Fr}_\ell^{-1})\gamma\left(\hat{d}'(x_{Sp^n}) - \hat{d}(x_{Sp^n})\right)\\
&= N_\ell\gamma\left(d_0(x_{S\ell p^n}) + a\right) - P_\ell(\mathrm{Fr}_\ell^{-1})\gamma\left(d_0(x_{Sp^n}) + a'\right)\\
&= N_\ell\gamma d_0(x_{S\ell p^n}) + N_\ell\gamma a - P_\ell(\mathrm{Fr}_\ell^{-1})\gamma d_0(x_{Sp^n}) - P_\ell(\mathrm{Fr}_\ell^{-1})\gamma a'\\
&= d_0\left(\gamma\left(N_\ell x_{S\ell p^n} - P_\ell(\mathrm{Fr}_\ell^{-1})x_{Sp^n}\right)\right) + N_\ell\gamma a - P_\ell(\mathrm{Fr}_\ell^{-1})\gamma a'\\
&= N_\ell\gamma a - P_\ell(\mathrm{Fr}_\ell^{-1})\gamma a'.
\end{aligned}$$

Since $\sigma_\ell \in \mathscr{I}_\ell$ fixes $E[q]$ and $q|\ell - 1$, we have $N_\ell\gamma a = 0$. We also have

$$P_\ell(\mathrm{Fr}_\ell^{-1})\gamma a' = \mathrm{Fr}_\ell^{-2}(\mathrm{Fr}_\ell^2 - a_\ell\mathrm{Fr}_\ell + \ell)\gamma a' = 0 \text{ in } E[q].$$

Thus, we prove the claim.

By the claim, we may replace $d_{S\ell p^n}$. We take $d_{S\ell p^n}$ as follows. We fix a positive integer k such that Fr_ℓ^k acts trivially on $\mathbb{Q}(Sp^n)$ and $E[q]$. Let k_p the largest power of p dividing k. We pick an integer $m \geq n$ such that the decomposition group of ℓ in $\mathbb{Q}(S\ell p^m)/\mathbb{Q}(S\ell p^n)$ has order divisible by $k_p q$. Let $d_{S\ell p^m} : X_{S\ell p^m} \to M_q/E[q]$ be a homomorphism of $\Gamma_{S\ell p^m}$-modules as in Proposition 4.2.18. Let $d_{S\ell p^n} : X_{S\ell p^n} \to M_q/E[q]$ be the composition

$$X_{S\ell p^n} \longrightarrow X_{S\ell p^m} \xrightarrow{d_{S\ell p^m}} M_q/E[q],$$

where the first homomorphism is induced by the map $x_{S'p^n} \mapsto \sum_{\sigma\in\mathrm{Gal}(\mathbb{Q}(p^m)/\mathbb{Q}(p^n))} \sigma x_{S'p^m}$ for $S'|S\ell$. We note that $\mathrm{Im}(d_{S\ell p^n}) \subseteq (M_q/E[q])^{G_{\mathbb{Q}(S\ell p^n)}}$. For $S'|S\ell$, we have

$$\begin{aligned}
\delta_{\mathbb{Q}(S\ell p^n)}(d_{S\ell p^n}(x_{S'p^n})) &= \delta_{\mathbb{Q}(S\ell p^n)}\left(d_{S\ell p^m}\left(\sum_{\sigma\in\mathrm{Gal}(\mathbb{Q}(p^m)/\mathbb{Q}(p^n))} \sigma x_{S'p^m}\right)\right)\\
&= \delta_{\mathbb{Q}(S\ell p^n)}\left(\sum_{\sigma\in\mathrm{Gal}(\mathbb{Q}(p^m)/\mathbb{Q}(p^n))} \sigma d_{S\ell p^m}\left(x_{S'p^m}\right)\right)\\
&= \mathrm{Cor}_{S'p^m/S'p^n}\left(\delta_{\mathbb{Q}(S\ell p^m)}(d_{S\ell p^m}(x_{S'p^m}))\right)\\
&= \mathrm{Cor}_{S'p^m/S'p^n}(z_{S'p^m})\\
&= z_{S'p^n}.
\end{aligned}$$

Thus, we deduce that $d_{S\ell p^n}$ satisfies the condition in Proposition 4.2.18.

Let $H \subset \mathrm{Gal}(\mathbb{Q}(S\ell p^m)/\mathbb{Q}(S\ell p^n))$ be the subgroup generated by Fr_ℓ^k. We fix a set $B \subset G_{\mathbb{Q}(S\ell p^n)}$ of coset representatives of $\mathrm{Gal}(\mathbb{Q}(S\ell p^m)/\mathbb{Q}(S\ell p^n))/H$. We put

$$N' = \sum_{i=0}^{|H|-1} \mathrm{Fr}_\ell^{ik} \in \mathbb{Z}[\mathscr{D}_\ell], \quad N'' = \sum_{\beta \in B} \beta \quad \in \mathbb{Z}[G_{\mathbb{Q}(S\ell p^n)}].$$

We note that

$$N'N'' = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(S\ell p^m)/\mathbb{Q}(S\ell p^n))} \sigma \quad \text{in} \quad \mathbb{Z}[\Gamma_{S\ell p^m}]. \tag{4.2.13}$$

We fix lifts $\hat{d}(x_{S\ell p^m})$, $\hat{d}(x_{Sp^m}) \in M_q$ of $d_{S\ell p^m}(x_{S\ell p^m}), d_{S\ell p^m}(x_{Sp^n})$, respectively. Since $d_{S\ell p^m}(x_{S\ell p^m}), d_{S\ell p^m}(x_{Sp^n}) \in (M_q/E[q])^{G_{\mathbb{Q}(S\ell p^m)}}$, by (4.2.13)

$$\hat{d}(x_{S\ell p^n}) := \gamma^{-1}N'N''\gamma\hat{d}(x_{S\ell p^m}), \quad \hat{d}(x_{Sp^n}) := \gamma^{-1}N'N''\gamma\hat{d}(x_{Sp^m}) \in M_q$$

are lists of $d_{S\ell p^n}(x_{S\ell p^n}), d_{S\ell p^n}(x_{Sp^n})$, respectively. We note that

$$N_\ell N''\hat{d}(x_{S\ell p^m}) - P_\ell(\mathrm{Fr}_\ell^{-1})N''\hat{d}(x_{Sp^m}) = 0 \ \text{ in } \ (M_q/E[q])^{G_{\mathbb{Q}(S\ell p^m)}}.$$

By Lemma 4.2.19, we have

$$\begin{aligned} &N_\ell\gamma\hat{d}(x_{S\ell p^n}) - P_\ell(\mathrm{Fr}_\ell^{-1})\gamma\hat{d}(x_{Sp^n}) \\ &= N_\ell N'N''\gamma\hat{d}(x_{S\ell p^m}) - P_\ell(\mathrm{Fr}_\ell^{-1})N'N''\gamma\hat{d}(x_{Sp^m}) \\ &= N'(N_\ell N''\hat{d}(x_{S\ell p^m}) - P_\ell(\mathrm{Fr}_\ell^{-1})N''\hat{d}(x_{Sp^m})) \\ &\in N'E[q]. \end{aligned}$$

Since Fr_ℓ^k fixes $E[q]$, we have

$$N'E[q] \subset |H|E[q].$$

Then, we are reduced to showing that q divides $|H|$.

We note that $\mathrm{Gal}(\mathbb{Q}(S\ell p^m)/\mathbb{Q}(S\ell p^n)) = \mathrm{Gal}(\mathbb{Q}(p^m)/\mathbb{Q}(p^n))$ is a cyclic group. Hence, if we denote by G the decomposition group of ℓ in $\mathrm{Gal}(\mathbb{Q}(S\ell p^m)/\mathbb{Q}(S\ell p^n))$, then by the definition of H we have

$$[G : H]|k_p.$$

On the other hand, we recall that $|G|$ is divisible by $k_p q$. Hence, we deuce that q divides $|H|$. □

We denote by $H^1_f(\mathbb{Q}_\ell, E[q])$ the image of the Kummer map $E(\mathbb{Q}_\ell)/q \hookrightarrow H^1(\mathbb{Q}_\ell, E[q])$, and put

$$H^1_{/f}(\mathbb{Q}_\ell, E[q]) = H^1(\mathbb{Q}_\ell, E[q])/H^1_f(\mathbb{Q}_\ell, E[q]),$$

which is isomorphic to $H^1(\mathbb{Q}_\ell, E)[q]$. By Proposition 2.1.2, we have

$$H^1_f(\mathbb{Q}_\ell, E[q]) = H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, E[q]),$$

and hence $H^1_{/f}(\mathbb{Q}_\ell, E[q]) = H^1(\mathbb{Q}_\ell^{\mathrm{ur}}, E[q])$. Then, we have two isomorphisms

$$\begin{aligned}
&\alpha_\ell : H^1_{/f}(\mathbb{Q}_\ell, E[q]) \cong E[q]^{\mathrm{Fr}_\ell = 1}; \quad c \mapsto c(\sigma_\ell), \\
&\beta_\ell : H^1_f(\mathbb{Q}_\ell, E[q]) \cong E[q]/(\mathrm{Fr}_\ell - 1)E[q]; \quad c \mapsto c(\mathrm{Fr}_q),
\end{aligned}$$

where each element $c \in H^1(\mathbb{Q}_\ell, E[q])$ is regarded as a cocycle. Here, we note that the map α_ℓ depends on the choice of σ_ℓ and coincides with the composite

$$H^1_{/f}(\mathbb{Q}_\ell, E[q]) \cong H^1(\mathbb{Q}_\ell^{\mathrm{ur}}, E[q])^{\mathrm{Fr}_\ell = 1} = \mathrm{Hom}_{\mathbb{Z}/q\mathbb{Z}}(\mathscr{I}_\ell/\mathscr{I}_\ell^q, E[q])^{\mathrm{Fr}_\ell = 1} \cong E[q]^{\mathrm{Fr}_\ell = 1},$$

where the last map is given by $c \mapsto c(\sigma_\ell)$.

Since $P_\ell(1) = 2 - a_\ell \equiv 0 \mod q$, we have $a_\ell \equiv 2 \mod q$, and hence

$$P_\ell(t) \equiv 1 - 2t + t^2 \equiv (t-1)^2 \mod q.$$

We put $Q_\ell(t) = t - 1 \in \mathbb{Z}/q\mathbb{Z}[t]$.

Since $P_\ell(t) \equiv \det_{\mathbb{Z}_p}(1 - \mathrm{Fr}_\ell t | T) \mod q$, we have

$$P_\ell(\mathrm{Fr}_\ell^{-1})E[q] = 0.$$

Therefore, since $P_\ell(t) \mod q = (t-1)Q_\ell(t)$, we have a homomorphism

$$Q_\ell(\mathrm{Fr}_\ell^{-1}) : E[q]/(\mathrm{Fr}_\ell - 1)E[q] \to E[q]^{\mathrm{Fr}_\ell = 1}.$$

We define

$$\phi_\ell^{fs} : H^1_f(\mathbb{Q}_\ell, E[q]) \to H^1_{/f}(\mathbb{Q}_\ell, E[q])$$

as the composite

$$H^1_f(\mathbb{Q}_\ell, E[q]) \xrightarrow{\beta_\ell} E[q]/(\mathrm{Fr}_\ell - 1)E[q] \xrightarrow{Q_\ell(\mathrm{Fr}_\ell^{-1})} E[q]^{\mathrm{Fr}_\ell = 1} \xrightarrow{\alpha_\ell^{-1}} H^1_{/f}(\mathbb{Q}_\ell, E[q]).$$

For each Darmon-Kolyvagin derivative D, we fix a lift D to $\mathbb{Z}[G_\mathbb{Q}]$.

Theorem 4.2.21. *Let S be an element of $\mathscr{N}_p$ and q a power of p. We take a prime $\ell \in \mathscr{R}_{E,q}$ which splits completely in $\mathbb{Q}(S)$. Let λ be the prime of $\mathbb{Q}(S)$ above ℓ corresponding to the decomposition group $\mathscr{D}_\ell$ of $\mathbb{Q}$. For a Darmon-Kolyvagin derivative D whose support is S, we have the following.*

1. $\mathrm{loc}_\lambda(Dz_S) \in H^1_f(\mathbb{Q}(S)_\lambda, E[q])$

2. $DD_\ell^{(1)} z_{S\ell} \in H^0\left(\Gamma_\ell, H^1(\mathbb{Q}(S\ell), T)/q\right)$.

3. *If* $\kappa^{(\ell)} \in H^1(\mathbb{Q}(S), E[q])$ *denotes the inverse image of* $DD_\ell^{(1)} z_{S\ell}$ *under the isomorphism* $H^1(\mathbb{Q}(S), E[q]) \cong H^0\left(\Gamma_\ell, H^1(\mathbb{Q}(S\ell), E[q])\right)$ *and* $\mathrm{loc}_{/f,\lambda}(\kappa^{(\ell)})$ *denotes the image of* $\kappa^{(\ell)}$ *in* $H^1_{/f}(\mathbb{Q}_\ell, E[q])$, *then we have*

$$\mathrm{loc}_{/f,\lambda}(\kappa^{(\ell)}) = \phi_\ell^{fs}(\mathrm{loc}_\lambda(Dz_S)).$$

Proof. The assertion 1 follows from Proposition 4.2.9.

By Lemma 4.1.1, we have

$$(\sigma_\ell - 1)DD_\ell^{(1)} x_{S\ell} \equiv -\sigma_\ell D N_\ell x_{S\ell} \equiv -\sigma_\ell D P_\ell(\mathrm{Fr}_\ell^{-1}) x_S \equiv -\sigma_\ell D P_\ell(1) x_S \equiv 0 \mod qX_{S\ell},$$

where the third congruence follows from $\mathrm{Fr}_\ell = 1$ in Γ_S, and the last congruence follows from $\ell \in \mathscr{R}_{E,q}$. Hence, $DD_\ell^{(1)} x_{S\ell} \in (X_{S\ell}/q)^{\Gamma_\ell}$. Since the homomorphism $d_{S\ell}$ as in Proposition 4.2.18 is $G_\mathbb{Q}$-equivariant, we have $d_{S\ell}(DD_\ell^{(1)} x_{S\ell}) \in (M_q/E[q])^{G_{\mathbb{Q}(S)}}$. Since $\delta_{\mathbb{Q}(S\ell)}(d_{S\ell}(x_{S\ell})) = z_{S\ell}$, by the commutative diagram

$$\begin{array}{ccc} (M_q/E[q])^{G_{\mathbb{Q}(S)}} & \xrightarrow{\delta_{\mathbb{Q}(S)}} & H^1(\mathbb{Q}(S), E[q]) \\ \downarrow \subseteq & & \downarrow \mathrm{res} \\ (M_q/E[q])^{G_{\mathbb{Q}(S\ell)}} & \xrightarrow{\delta_{\mathbb{Q}(S\ell)}} & H^1(\mathbb{Q}(S\ell), E[q]), \end{array}$$

we have $\mathrm{res}(\delta_{\mathbb{Q}(S)}(d_{S\ell}(DD_\ell^{(1)} x_{S\ell}))) = DD_\ell^{(1)} z_{S\ell}$ and hence

$$DD_\ell^{(1)} z_{S\ell} \in H^0\left(\Gamma_\ell, H^1(\mathbb{Q}(S\ell), T)/q\right).$$

We take lifts $\hat{d}(x_{S\ell}), \hat{d}(x_S) \in M_q$ of $d_{S\ell}(x_{S\ell}), d_{S\ell}(x_S)$, respectively. According to the definition of ϕ_ℓ^{fs}, it suffices to show that

$$Q_\ell(\mathrm{Fr}_\ell^{-1})\left((Dz_S)(\mathrm{Fr}_\ell)\right) = \kappa^{(\ell)}(\sigma_\ell) \in E[q]. \tag{4.2.14}$$

Since $\delta_{\mathbb{Q}(S)}(d_{S\ell}(x)) = z_S$, $\delta_{\mathbb{Q}(S)}(D_\ell^{(1)} D(d_{S\ell}(x)) = \kappa^{(\ell)}$ and $\delta_{\mathbb{Q}(S)}$ is the connecting map from $(M_q/E[q])^{G_{\mathbb{Q}(S)}}$ to $H^1(\mathbb{Q}(S), E[q])$, we have

$$\begin{aligned} (Dz_S)(\mathrm{Fr}_\ell) &= (\mathrm{Fr}_\ell - 1)D\hat{d}(x_S) \in E[q], \\ \kappa^{(\ell)}(\sigma_\ell) &= (\sigma_\ell - 1)D_\ell^{(1)} D\hat{d}(x_{S\ell}) \in E[q]. \end{aligned} \tag{4.2.15}$$

Since $P_\ell(\mathrm{Fr}_\ell^{-1})E[q] = 0$, we have $Q_\ell(\mathrm{Fr}_\ell^{-1})(\mathrm{Fr}_\ell^{-1} - 1)\left((Dz_S)(\mathrm{Fr}_\ell)\right) = 0$, and hence

$$Q_\ell(\mathrm{Fr}_\ell^{-1})\left((Dz_S)(\mathrm{Fr}_\ell)\right) = Q_\ell(\mathrm{Fr}_\ell^{-1})\mathrm{Fr}_\ell^{-1}\left((Dz_S)(\mathrm{Fr}_\ell)\right).$$

Thus, by (4.2.15), (4.2.11) and Lemma 4.2.19, we obtain

$$Q_\ell(\mathrm{Fr}_\ell^{-1})((Dz_S)(\mathrm{Fr}_\ell)) - \kappa^{(\ell)}(\sigma_\ell)$$

$$\begin{aligned}
&= Q_\ell(\mathrm{Fr}_\ell^{-1})\mathrm{Fr}_\ell^{-1}((Dz_S)(\mathrm{Fr}_\ell)) - \kappa^{(\ell)}(\sigma_\ell) \\
&= Q_\ell(\mathrm{Fr}_\ell^{-1})\mathrm{Fr}_\ell^{-1}(\mathrm{Fr}_\ell - 1)D\hat{d}(x_S) - (\sigma_\ell - 1)D_\ell^{(1)}D\hat{d}(x_{S\ell}) \\
&= -P_\ell(\mathrm{Fr}_\ell^{-1})D\hat{d}(x_S) + N_\ell D\hat{d}(x_{S\ell}).
\end{aligned}$$

By Lemma 4.2.20, we conclude (4.2.14). □

Lemma 4.2.22. *If $E[q]/(\mathrm{Fr}_\ell - 1)E[q]$ is free of rank one over $\mathbb{Z}/q\mathbb{Z}$, then*

$$Q_\ell(\mathrm{Fr}_\ell^{-1}) : E[q]/(\mathrm{Fr}_\ell - 1)E[q] \to E[q]^{\mathrm{Fr}_\ell = 1}$$

is an isomorphism.

Proof. By the exact sequence

$$0 \to E[q]^{\mathrm{Fr}_\ell=1} \to E[q] \xrightarrow{\mathrm{Fr}_\ell - 1} E[q] \to E[q]/(\mathrm{Fr}_\ell - 1)E[q] \to 0,$$

we also have

$$E[q]^{\mathrm{Fr}_\ell=1} \cong \mathbb{Z}/q\mathbb{Z}.$$

We take a $\mathbb{Z}/q\mathbb{Z}$-basis $\{P_1, P_2\}$ of $E[q]$ such that $\mathrm{Fr}_\ell P_1 \neq P_1$ and $\mathrm{Fr}_\ell P_2 = P_2$. Then, we have

$$\mathrm{Fr}_\ell \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix},$$

where $a, b \in \mathbb{Z}/q\mathbb{Z}$. Since $\det_{\mathbb{Z}/q\mathbb{Z}}(E[q]) \cong \mu_q$ as a $G_{\mathbb{Q}_\ell}$-module and Fr_ℓ acts trivially on μ_q, we obtain

$$\det \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} = 1.$$

Hence, we have $a = 1$ and

$$(\mathrm{Fr}_\ell - 1)E[q] = b\mathbb{Z}/q\mathbb{Z}P_2.$$

Therefore, since $E[q]/(\mathrm{Fr}_\ell - 1)E[q] \cong \mathbb{Z}/q\mathbb{Z}$, we have $b \in (\mathbb{Z}/q\mathbb{Z})^\times$. Hence, we have

$$Q_\ell(\mathrm{Fr}_\ell^{-1})E[q] = (\mathrm{Fr}_\ell^{-1} - 1)E[q] = -\mathrm{Fr}_\ell^{-1}(\mathrm{Fr}_\ell - 1)E[q] = \mathbb{Z}/q\mathbb{Z}P_2,$$

which shows that $Q_\ell(\mathrm{Fr}_\ell^{-1}) : E[q] \to E[q]^{\mathrm{Fr}_\ell=1}$ is surjective. Thus, by comparing orders, we deduce that the map

$$Q_\ell(\mathrm{Fr}_\ell^{-1}) : E[q]/(\mathrm{Fr}_\ell - 1)E[q] \to E[q]^{\mathrm{Fr}_\ell=1}$$

is an isomorphism. □

Corollary 4.2.23. *Under the notation in Theorem 4.2.21, if $E[q]/(\mathrm{Fr}_\ell - 1)E[q] \cong \mathbb{Z}/q\mathbb{Z}$ then we have*

$$\mathrm{ord}(\mathrm{loc}_\lambda(\kappa^{(\ell)}), H^1(\mathbb{Q}_\ell, E)[q]) = \mathrm{ord}(\mathrm{loc}_\lambda(Dz_S), H^1(\mathbb{Q}_\ell, E[q])).$$

Proof. By Lemma 4.2.22, the homomorphism ϕ_ℓ^{fs} is an isomorphism. Then, the corollary follows from the assertion 3 of Theorem 4.2.21. □

4.3 The theorem on divisibility of Euler systems

The aim of this section is to prove Theorem 4.3.10. It suggests congruences of derivatives of Euler systems, and plays an important role in the proof of our main result (Theorem 5.4.1). We also give a modification (Theorem 4.3.15) of Theorem 4.3.10, which is used to prove Theorems 4.5.2 and 5.4.2.

As in Section 4.2, we denote by E an elliptic curve over $\mathbb{Q}$ of conductor N without complex multiplication. We fix an Euler system $\{z_{Sp^n}\}_{S\in\mathscr{N},n\geq 0}$ for $T = T_p(E)$ in the sense of Definition 4.2.6.

4.3.1 Notation

Assumption 4.3.1. In the following, we assume that

1. $p \nmid 6N\prod_{\ell|N} m_\ell$,
2. the Galois representation $G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_p}(T)$ is surjective.

Let q be a power of p.

Definition 4.3.2. For a finitely generated $\mathbb{Z}_p$-module M, we define a non-negative integer $r_q(M)$ by

$$M \otimes \mathbb{Z}/q\mathbb{Z} \cong (\mathbb{Z}/q\mathbb{Z})^{\oplus r_q(M)} \oplus M',$$

where the exponent of M' is strictly less than q.

We have a basic property:

Lemma 4.3.3. *For an exact sequence of finite $\mathbb{Z}/q\mathbb{Z}$-modules*

$$0 \to M' \to M \to M'',$$

we have

$$r_q(M) \leq r_q(M') + r_p(M'').$$

Proof. We denote by f the map from M to M''. Since $r_p(f(M)) \leq r_p(M'')$, by replacing M'' with $f(M)$ we may assume that f is surjective. We write $q = p^m$. Then, there is an exact sequence

$$0 \to p^{m-1}M' \to p^{m-1}M \to M''/f(M[p^{m-1}]), \tag{4.3.1}$$

where the last morphism is given by $p^{m-1}a \mapsto f(a)$ for $a \in M$. Since

$$M''/f(M[p^{m-1}]) = f(M)/f(M[p^{m-1}])$$

is an $\mathbb{F}_p$-vector space, the sequence (4.3.1) is an exact sequence of $\mathbb{F}_p$-vector spaces. Therefore, we have

$$\dim_{\mathbb{F}_p}(p^{m-1}M) \leq \dim_{\mathbb{F}_p}(p^{m-1}M') + \dim_{\mathbb{F}_p}(M''/f(M[p^{m-1}]).$$

By definition, we have

$$r_q(M) = \dim_{\mathbb{F}_p}(p^{m-1}M),\ r_q(M') = \dim_{\mathbb{F}_p}(p^{m-1}M'),\ \dim_{\mathbb{F}_p}(M''/f(M[p^{m-1}]) \leq r_p(M'').$$

Thus, we complete the proof. □

Definition 4.3.4. For a positive integer S, we define $H^1_{f,S}(\mathbb{Q}, E[q])$ by

$$H^1_{f,S}(\mathbb{Q}, E[q]) = \ker\left(\mathrm{Sel}(\mathbb{Q}, E[q]) \to \oplus_{\ell|S} E(\mathbb{Q}_\ell)/q\right), \tag{4.3.2}$$

where ℓ ranges over all the primes dividing S. If there is no fear of confusion, we simply write $H^1_{f,S} = H^1_{f,S}(\mathbb{Q}, E[q])$.

We put

$$A_q(S) = \oplus_{\ell|S} E(\mathbb{Q}_\ell)/q.$$

Lemma 4.3.5. *Let S be a positive integer and $\ell \nmid S$ a prime such that $E(\mathbb{Q}_\ell)/p$ is cyclic (i.e. $E(\mathbb{Q}_\ell)/p$ is trivial or isomorphic to $\mathbb{Z}/p\mathbb{Z}$. See Proposition 2.1.1). Then, we have*

$$r_q(H^1_{f,S\ell}) + r_p(A_q(S\ell)) - 1 \leq r_q(H^1_{f,S}) + r_p(A_q(S)). \tag{4.3.3}$$

In addition, if $E(\mathbb{Q}_\ell)/p \cong \mathbb{Z}/p$, then we have

$$r_q(H^1_{f,S}) + r_p(A_q(S)) \leq r_q(H^1_{f,S\ell}) + r_p(A_q(S\ell)) \tag{4.3.4}$$

Proof. Since $H^1_{f,S\ell} \subseteq H^1_{f,S}$, $r_p(A_q(S\ell)) \leq r_p(A_q(S)) + 1$, we have the first inequality. We assume that $E(\mathbb{Q}_\ell)/p \cong \mathbb{Z}/p$. By the exact sequence

$$0 \to H^1_{f,S\ell} \to H^1_{f,S} \to E(\mathbb{Q}_\ell)/q$$

and Lemma 4.3.3, we have

$$r_q(H^1_{f,S}) \leq r_q(H^1_{f,S\ell}) + r_p(E(\mathbb{Q}_\ell)/p) = r_q(H^1_{f,S\ell}) + 1.$$

Since $r_p(A_q(S)) + 1 = r_p(A_q(S\ell))$, we conclude

$$r_q(H^1_{f,S}) + r_p(A_q(S)) \leq r_q(H^1_{f,S\ell}) + r_p(A_q(S\ell)).$$

□

Definition 4.3.6. Let $S \in \mathscr{N}_q$ (see (4.2.5) for $\mathscr{N}_q$). For a Darmon-Kolyvagin derivative D whose support is S, we define the *weight* of D as

$$w(D) = \mathrm{ord}(D) - |\{\ell \in \mathscr{R}_{E,q};\ \ell \text{ divides } S\}|.$$

Remark 4.3.7. In Darmon's argument, the notion of weight also played an important role. We modify his weight for our case.

Definition 4.3.8. For a positive integer m, we denote by $\nu(m)$ the number of primes dividing m.

Proposition 4.3.9. *Let D be a Darmon-Kolyvagin derivative with support S. Suppose that $S \in \mathscr{N}_q$. If $w(D) < 0$ and $\max_{\ell|S}\{e_\ell(D)\} < p$ (see Definition 4.1.2 for $e_\ell(D)$), then we have*

$$Dz_S \equiv 0 \mod qH^1(\mathbb{Q}(S), T).$$

Proof. We note that the assumption $w(D) < 0$ implies that there exist a prime $\ell \in \mathscr{R}_{E,q}$ dividing S and derivative D' such that

$$D = D'N_\ell \quad \mathrm{Supp}(D') = S/\ell, \quad \mathrm{ord}(D') = \mathrm{ord}(D). \tag{4.3.5}$$

We prove the proposition by induction on $\nu(S)$. If $S = \ell$ is a prime, then $\ell \in \mathscr{R}_{E,q}$ and $D = N_\ell$. Hence, since $P_\ell(1) \equiv 0 \mod q$,

$$Dz_\ell = N_\ell z_\ell = P_\ell(\mathrm{Fr}_\ell^{-1})z_1 \equiv P_\ell(1)z_1 \equiv 0 \mod q.$$

In general, since $w(D) < 0$, there exists a prime $\ell \in \mathscr{R}_{E,q}$ dividing S, and we define D' as in (4.3.5). Then, we have

$$\begin{aligned} w(D') &= \mathrm{ord}(D') - |\{\ell' \in \mathscr{R}_{E,q};\ \ell' \text{ divides } S/\ell\}| \\ &= \mathrm{ord}(D) - |\{\ell' \in \mathscr{R}_{E,q};\ \ell' \text{ divides } S\}| + 1 \\ &= w(D) + 1 \leq 0. \end{aligned}$$

We write $S/\ell = \ell_1 \cdots \ell_a$. We show that

$$(\sigma_{\ell_i} - 1)D'z_{S/\ell} \equiv 0 \mod q \quad \text{for } 1 \leq i \leq a \tag{4.3.6}$$

It suffices to consider the case $i = 1$. We write $D' = D_{\ell_1}^{(k_1)} \cdots D_{\ell_a}^{(k_a)}$. If $k_1 = 0$, then $D' = N_{\ell_1} D_{\ell_2}^{(k_2)} \cdots D_{\ell_a}^{(k_a)}$. Hence (4.3.6) is clear. We may assume that $k_i \geq 1$. Since the order of σ_{ℓ_1} is divisible by q and $0 < k_1 < p$, Lemma 4.1.1 implies that

$$(\sigma_{\ell_1} - 1)D' \equiv -\sigma_{\ell_1} D_{\ell_1}^{(k_1-1)} D_{\ell_2}^{(k_2)} \cdots D_{\ell_a}^{(k_a)} \mod q. \tag{4.3.7}$$

We have

$$\mathrm{Supp}(D_{\ell_1}^{(k_1-1)}D_{\ell_2}^{(k_2)}\cdots D_{\ell_a}^{(k_a)}) = S/\ell, \quad w(D_{\ell_1}^{(k_1-1)}D_{\ell_2}^{(k_2)}\cdots D_{\ell_a}^{(k_a)}) = w(D') - 1 < 0.$$

By the induction hypothesis,

$$D_{\ell_1}^{(k_1-1)}D_{\ell_2}^{(k_2)}\cdots D_{\ell_a}^{(k_a)} z_{S/\ell} \equiv 0 \mod q,$$

and hence by (4.3.7),

$$(\sigma_{\ell_1} - 1)D' z_{S/\ell} \equiv 0 \mod q.$$

Since Γ_{ℓ_1} is generated by σ_{ℓ_1}, we have $D' z_{S/\ell} \in H^0\left(\Gamma_{\ell_1}, H^1(\mathbb{Q}(S/\ell), T)/q\right)$. Then, we show (4.3.6), and obtain

$$D' z_{S/\ell} \in H^0\left(\Gamma_{S/\ell}, H^1(\mathbb{Q}(S/\ell), T)/q\right).$$

Therefore, since $P_\ell(1) \equiv 0 \mod q$, we have

$$Dz_S = D'N_\ell z_S = P_\ell(\mathrm{Fr}_\ell^{-1})D' z_{S/\ell} \equiv P_\ell(1)D' z_{S/\ell} \equiv 0 \mod q.$$

□

4.3.2 The proof and an application

Now, we state our theorem on congruences of derivatives.

Theorem 4.3.10. *Let q be a power of p. Let D be a Darmon-Kolyvagin derivative with support S satisfying $\max_{\ell|S}\{e_\ell(D)\} < p$. We suppose that $S \in \mathscr{N}_q$ and for every prime $\ell|S$, $E(\mathbb{F}_\ell)[p]$ is cyclic, that is, $E(\mathbb{F}_\ell)[p] = 0$ or $E(\mathbb{F}_\ell)[p] \cong \mathbb{Z}/p\mathbb{Z}$ (cf. (2.1.1)). If $\mathrm{ord}(D) < r_q\left(H^1_{f,p}(\mathbb{Q}, E[q])\right)$, then we have*

$$Dz_S \equiv 0 \mod qH^1(\mathbb{Q}(S), T).$$

We prove it by induction on $w(D)$. Before the proof, we prove a lemma.

Lemma 4.3.11. *We fix $w \in \mathbb{Z}$, and assume that Theorem 4.3.10 holds for any Darmon-Kolyvagin derivative whose weight is strictly less than w. Let D be a Darmon-Kolyvagin derivative with support S such that $\max_{\ell|S}\{e_\ell(D)\} < p$ and $w(D) = w$. We suppose that $S \in \mathscr{N}_q$ and $E(\mathbb{F}_\ell)[p]$ is cyclic for every prime $\ell|S$. If $\mathrm{ord}(D) < r_q\left(H^1_{f,p}(\mathbb{Q}, E[q])\right)$, then the following assertions hold.*

1. *We have*

$$Dz_S \in H^0\left(\Gamma_S, H^1(\mathbb{Q}(S), T)/q\right).$$

2. *We take a prime $\ell \in \mathscr{R}_{E,q}$ which splits completely in $\mathbb{Q}(S)$, and suppose that $E(\mathbb{Q}_\ell)/q \cong \mathbb{Z}/q\mathbb{Z}$. Then, we have*

$$DD_\ell^{(1)} z_{S\ell} \in H^0\left(\Gamma_{S\ell}, H^1(\mathbb{Q}(S\ell), T)/q\right).$$

PROOF. We write $S = \ell_1 \cdots \ell_s$. We first show the assertion 1. It suffices to show that

$$Dz_S \in H^0\left(\Gamma_{\ell_i}, H^1(\mathbb{Q}(S), T)/q\right) \tag{4.3.8}$$

for each $1 \leq i \leq s$.

It suffices to consider the case $i = 1$. If $e_{\ell_1}(D) = 0$, then we have $D = N_{\ell_1} D'$ for some derivative D'. Since $(\sigma_{\ell_1} - 1)N_{\ell_1} = 0$, we prove (4.3.8). Then, we may assume that $e_{\ell_1}(D) \geq 1$. By Lemma 4.1.1, we have

$$(\sigma_{\ell_1} - 1)D \equiv -\sigma_{\ell_1} D' \mod q\mathbb{Z}[\Gamma_S],$$

where D' is a derivative such that

$$\mathrm{ord}(D') = \mathrm{ord}(D) - 1, \quad \mathrm{Supp}(D') = S.$$

Then, we have

$$\begin{aligned} w(D') &= \mathrm{ord}(D') - |\{\ell' \in \mathscr{R}_{E,q};\ \ell' \text{ divides } S\}| \\ &= \mathrm{ord}(D) - 1 - |\{\ell' \in \mathscr{R}_{E,q};\ \ell' \text{ divides } S\}| \\ &= w(D) - 1 = w - 1, \end{aligned}$$

which shows that Theorem 4.3.10 holds for D', that is, $D'z_S \equiv 0 \mod qH^1(\mathbb{Q}(S), T)$. Hence, we obtain

$$(\sigma_{\ell_1} - 1)Dz_S \equiv -\sigma_{\ell_1} D' z_S \equiv 0 \mod q,$$

which shows (4.3.8). Hence, we prove the assertion 1.

Next, we show the assertion 2. Since $(\sigma_\ell - 1)DD_\ell^{(1)} \equiv -\sigma_\ell D N_\ell \mod q$ and $\mathrm{Fr}_\ell = 1$ in Γ_S, we have

$$(\sigma_\ell - 1)DD_\ell^{(1)} z_{S\ell} \equiv -\sigma_\ell D N_\ell z_{S\ell} \equiv -DP_\ell(\mathrm{Fr}_\ell^{-1}) z_S \equiv -DP_\ell(1) z_S \equiv 0 \mod q. \tag{4.3.9}$$

Then, we are reduced to proving that

$$DD_\ell^{(1)} z_{S\ell} \in H^0\left(\Gamma_{\ell_i}, H^1(\mathbb{Q}(S\ell), T)/q\right) \tag{4.3.10}$$

for each $1 \leq i \leq s$.

We only need to consider the case $i = 1$. In the case where $e_{\ell_1}(D) = 0$, we have $D \in N_{\ell_1}\mathbb{Z}[\Gamma_S]$, and hence we have (4.3.10). We assume that $e_{\ell_1}(D) \geq 1$. By Lemma 4.1.1, we have

$$(\sigma_{\ell_1} - 1)D \equiv -\sigma_{\ell_1} D' \mod q\mathbb{Z}[\Gamma_S],$$

where D' is a derivative such that

$$\mathrm{ord}(D') = \mathrm{ord}(D) - 1, \quad \mathrm{Supp}(D') = S.$$

We have

$$\begin{aligned} w(D'D_\ell^{(1)}) &= \mathrm{ord}(D'D_\ell^{(1)}) - |\{\ell' \in \mathscr{R}_{E,q};\ \ell' \text{ divides } S\ell\}| \\ &= \mathrm{ord}(D) - |\{\ell' \in \mathscr{R}_{E,q};\ \ell' \text{ divides } S\}| - 1 \\ &= w(D) - 1 = w - 1. \end{aligned}$$

Therefore, Theorem 4.3.10 holds for D', and hence $D'D_\ell^{(1)} z_{S\ell} \equiv 0 \mod q$. From this, we have

$$(\sigma_{\ell_i} - 1)DD_\ell^{(1)} z_{S\ell} \equiv -\sigma_{\ell_i} D'D_\ell^{(1)} z_{S\ell} \equiv 0 \mod q,$$

which shows (4.3.10). We thus conclude the assertion 2. □

Proof of Theorem 4.3.10. We prove the theorem by induction on $w(D)$. Note that the theorem obviously follows from Proposition 4.3.9 when $w(D) < 0$. We may assume that $w := w(D) \geq 0$ and the theorem holds for any derivative whose weight is strictly less than w. We assume that

$$Dz_S \not\equiv 0 \mod q \tag{4.3.11}$$

to have a contradiction. We put $S' = \mathrm{Cond}(D)$.

Claim 1. We have

$$r_q\left(H^1_{f,pS'}(\mathbb{Q}, E[q])\right) > 0.$$

Proof of Claim 1. We assume that $r_q\left(H^1_{f,pS'}(\mathbb{Q}, E[q])\right) = 0$. By Lemma 4.3.3 and the exact sequence

$$0 \to H^1_{f,pS'}(\mathbb{Q}, E[q]) \to H^1_{f,p}(\mathbb{Q}, E[q]) \to \oplus_{\ell|S'} E(\mathbb{Q}_\ell)/q,$$

we have

$$r_q\left(H^1_{f,p}(\mathbb{Q}, E[q])\right) \leq r_q\left(H^1_{f,pS'}(\mathbb{Q}, E[q])\right) + r_p(\oplus_{\ell|S'} E(\mathbb{Q}_\ell)/p),$$

and hence by the assumption,

$$\mathrm{ord}(D) < \sum_{\ell|S'} r_p(E(\mathbb{Q}_\ell)/p).$$

By Proposition 2.1.1, for a prime $\ell \nmid pN$ we have

$$E(\mathbb{Q}_\ell)/p \cong E(\mathbb{F}_\ell)[p].$$

Since $E(\mathbb{F}_\ell)[p]$ is assumed to be cyclic for $\ell|S$, we have $r_p(E(\mathbb{Q}_\ell)/p) \leq 1$. Then we have

$$\mathrm{ord}(D) < \sum_{\ell|S'} 1.$$

However, by the definition of $S' = \mathrm{Cond}(D)$, we have $\sum_{\ell|S'} 1 \leq \mathrm{ord}(D)$. Then, we have a contradiction, and conclude the claim.

Proposition 4.2.1 asserts that the restriction map

$$H^1(\mathbb{Q}, E[q]) \to H^0\left(\Gamma_S, H^1(\mathbb{Q}(S), E[q])\right)$$

is an isomorphism. By Lemma 4.3.11, we have $Dz_S \in H^0\left(\Gamma_S, H^1(\mathbb{Q}(S), E[q])\right)$. We denote by $\kappa \in H^1(\mathbb{Q}, E[q])$ the inverse image of Dz_S under the restriction map above. By (4.3.11) and the exact sequence

$$H^1(\mathbb{Q}(S), T) \xrightarrow{\times q} H^1(\mathbb{Q}(S), T) \to H^1(\mathbb{Q}(S), T/q),$$

we have $\kappa \neq 0$.

Claim 2. There exists a good prime ℓ of E such that

(1) $\ell \equiv 1 \mod q$, ℓ splits in $\mathbb{Q}(S)$, and $E(\mathbb{Q}_\ell)/q \cong \mathbb{Z}/q\mathbb{Z}$ (in particular $\ell \in \mathscr{R}_{E,q}$),

(2) $\mathrm{loc}_\ell(\kappa) \neq 0$ in $H^1(\mathbb{Q}_\ell, E[q])$,

(3) the localization map $H^1_{f,pS'}(\mathbb{Q}, E[q]) \to E(\mathbb{Q}_\ell)/q$ is surjective.

Proof of Claim 2. By Claim 1, there exists an element $\eta \in H^1_{f,pS'}(\mathbb{Q}, E[q])$ of order q. We put $L = \mathbb{Q}(S)(E[q])$ (the composite of $\mathbb{Q}(S)$ and $\mathbb{Q}(E[q])$). Since $(S, pN) = 1$, we have $\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(E[q])/\mathbb{Q})$. By Proposition 4.2.2, we have

$$H^1(L/\mathbb{Q}(S), E[q]) \cong H^1(\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}), (\mathbb{Z}/q\mathbb{Z})^{\oplus 2}) = 0.$$

Hence, the restriction map

$$H^1(\mathbb{Q}(S), E[q]) \to H^1(L, E[q])$$

is injective, and then the restriction map $H^1(\mathbb{Q}, E[q]) \to H^1(L, E[q])$ is also injective. Then, the element κ is non-trivial and η is of order q in $H^1(L, E[q])$. By Lemma 4.2.4 we have an element γ of G_L such that

(4.3.12) $\kappa(\gamma\tau)$ is non-trivial and $\eta(\gamma\tau)$ is of order q in $E[q]/(\tau - 1)E[q]$,

where the element $\tau \in G_{\mathbb{Q}(\mu_{Sp^\infty})}$ is as in (4.2.1). We regard κ, η as elements of $H^1(L, E[q]) = \mathrm{Hom}(G_L, E[q])$, and put $H = \ker(\kappa) \cap \ker(\eta) \subset G_L$. Let L' be a finite Galois extension of $\mathbb{Q}$ containing $\overline{\mathbb{Q}}^H$. For $\sigma \in G_{\mathbb{Q}}$, we denote by $[\sigma]$ the conjugacy class of the image of σ in $\mathrm{Gal}(L'/\mathbb{Q})$. Then, by Chebotarev's density theorem, there exists a prime $\ell \nmid pNS$ such that

$$[\mathrm{Fr}_\ell] = [\gamma\tau]. \tag{4.3.13}$$

We show that this ℓ satisfies the conditions (1), (2) and (3) in Claim 2 above.

(1). Since $\gamma\tau = 1$ in $\mathrm{Gal}(\mathbb{Q}(S)(\mu_q)/\mathbb{Q})$ (recall that $\mathbb{Q}(\mu_q) \subseteq \mathbb{Q}(E[q])$ by the Weil pairing),

$$\ell \equiv 1 \mod q, \text{ and } \ell \text{ splits completely in } \mathbb{Q}(S).$$

By (4.3.13), we have $\mathrm{Fr}_\ell = \sigma\gamma\tau\sigma^{-1}$ in $\mathrm{Gal}(\mathbb{Q}(E[q])/\mathbb{Q})$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[q]/\mathbb{Q})$. Then, since $\gamma\tau = \tau$ in $\mathrm{Gal}(\mathbb{Q}(E[q])/\mathbb{Q})$ and (4.2.1), we have

$$H^1(\mathbb{F}_\ell, E[q]) \cong E[q]/(\mathrm{Fr}_\ell - 1)E[q] = E[q]/\sigma(\tau - 1)E[q] \cong \mathbb{Z}/q\mathbb{Z},$$

where the first isomorphism is given by $f \mapsto f(\mathrm{Fr}_\ell)$. Proposition 2.1.2 implies that

$$E(\mathbb{Q}_\ell)/q = H^1(\mathbb{F}_\ell, E[q]).$$

Hence we deduce that the condition (1) holds.

(2). By Proposition 4.2.10, the image $\mathrm{loc}_\ell(\kappa)$ belongs to $H^1(\mathbb{F}_\ell, E[q])$. By the isomorphism $H^1(\mathbb{F}_\ell, E[q]) \cong E[q]/(\mathrm{Fr}_\ell - 1)E[q]$, it suffices to show that for a lift $\mathrm{Fr}_\ell \in G_{\mathbb{Q}}$ of the arithmetic Frobenius at ℓ,

$$\kappa(\mathrm{Fr}_\ell) \neq 0. \tag{4.3.14}$$

By (4.3.13), we write $\mathrm{Fr}_\ell = \sigma\gamma\tau\sigma^{-1}g \in G_{\mathbb{Q}}$ for some $\sigma \in G_{\mathbb{Q}}$ and $g \in G_{L'}$. Then, for every $\xi \in H^1(\mathbb{Q}, E[q])$ which is unramified at ℓ such that $\xi(g) = 0$, we have

$$\begin{aligned}
\xi(\mathrm{Fr}_\ell) &= \xi(\sigma\gamma\tau\sigma^{-1}g) \overset{\text{(i)}}{=} \xi(\sigma\gamma\tau\sigma^{-1}) = \sigma\xi(\gamma\tau\sigma^{-1}) + \xi(\sigma) \\
&= \sigma(\gamma\tau\xi(\sigma^{-1}) + \xi(\gamma\tau)) + \xi(\sigma) \overset{\text{(ii)}}{=} \sigma\tau\xi(\sigma^{-1}) + \xi(\sigma) + \sigma\xi(\gamma\tau) \\
&= -\sigma\tau\sigma^{-1}\xi(\sigma) + \xi(\sigma) + \sigma\xi(\gamma\tau) = -(\mathrm{Fr}_\ell - 1)\xi(\sigma) + \sigma\xi(\gamma\tau) \\
&= \sigma\xi(\gamma\tau) \text{ in } E[q]/(\mathrm{Fr}_\ell - 1)E[q],
\end{aligned}$$

where the equality (i) follows from $\xi(g) = 0$, and (ii) follows from $\gamma \in G_L$. Since

$$(\mathrm{Fr}_\ell - 1)E[q] = \sigma(\tau - 1)E[q],$$

we obtain

$$\operatorname{ord}\left(\xi(\mathrm{Fr}_\ell), E[q]/(\mathrm{Fr}_\ell - 1)E[q]\right) = \operatorname{ord}\left(\xi(\gamma\tau), E[q]/(\tau - 1)E[q]\right). \tag{4.3.15}$$

By (4.3.12) and (4.3.15) with $\xi = \kappa$, we deduce (4.3.14).

(3). By definition, the image $\mathrm{loc}_\ell(\eta)$ belongs to $H^1(\mathbb{F}_\ell, E[q])$ By (4.3.12) and (4.3.15) with $\xi = \eta$, we deduce that $\operatorname{ord}\left(\eta(\mathrm{Fr}_\ell), E[q]/(\mathrm{Fr}_\ell - 1)E[q]\right) = q$, and hence the element $\mathrm{loc}_\ell(\eta) \in E(\mathbb{Q}_\ell)/q$ is of order q. Therefore, since $E(\mathbb{Q}_\ell)/q \cong \mathbb{Z}/q\mathbb{Z}$, we deduce the assertion (3).

By Lemma 4.3.11, we have

$$DD_\ell^{(1)} z_{S\ell} \in H^0\left(\Gamma_{S\ell}, H^1(\mathbb{Q}(S\ell), T)/q\right).$$

Let $\kappa^{(\ell)} \in H^1(\mathbb{Q}, E[q])$ denote the inverse image of $DD_\ell^{(1)} z_{S\ell} \in H^0\left(\Gamma_{S\ell}, H^1(\mathbb{Q}(S\ell), E[q])\right)$ under the isomorphism $H^1(\mathbb{Q}, E[q]) \cong H^0\left(\Gamma_{S\ell}, H^1(\mathbb{Q}(S\ell), E[q])\right)$.

Claim 3. We have $\mathrm{loc}_\ell(\kappa^{(\ell)}) \in H^1_f(\mathbb{Q}_\ell, E[q])$.

Proof of Claim 3. By taking the Pontryagin dual, Claim 2 (3) implies that the map

$$H^1(\mathbb{Q}_\ell, E)[q] \to H^1_{f,pS'}(\mathbb{Q}, E[q])^\vee; \quad a \mapsto (y \mapsto (y, a)_\ell) \tag{4.3.16}$$

is injective, where $(-,-)_\ell$ is the cup product $H^1(\mathbb{Q}_\ell, E[q]) \times H^1(\mathbb{Q}_\ell, E[q]) \to \mathbb{Z}/q\mathbb{Z}$. Hence, it suffices to show that the image of $\kappa^{(\ell)}$ in $H^1(\mathbb{Q}_\ell, E)[q]$ is in the kernel of the map above. For $x \in H^1_{f,pS'}(\mathbb{Q}, E[q])$, the Hasse principle shows that

$$(x, \kappa^{(\ell)})_\ell = -\sum_{w \nmid \ell : \text{prime}} (x, \kappa^{(\ell)})_w. \tag{4.3.17}$$

By Corollary 4.2.11, we have $\mathrm{loc}_w(\kappa^{(\ell)}) \in E(\mathbb{Q}_w)/q$ for $w \nmid pS'\ell$. Since the localization $\mathrm{loc}_w(x)$ at w belongs to $E(\mathbb{Q}_w)/q$,

$$(x, \kappa^{(\ell)})_w = 0$$

For $w | pS'$, by the definition of $H^1_{f,pS'}$, we have $(x, \kappa^{(\ell)})_w = 0$. Therefore by (4.3.17), we obtain $(x, \kappa^{(\ell)})_\ell = 0$. Since $x \in H^1_{f,pS'}(\mathbb{Q}, E[q])$ is arbitrary, we deduce that $\mathrm{loc}_\ell(\kappa^{(\ell)})$ is in the kernel of the map (4.3.16). Then, we have $\mathrm{loc}_\ell(\kappa^{(\ell)}) \in H^1_f(\mathbb{Q}_\ell, E[q])$.

On the other hand, Corollary 4.2.23 shows that

$$\operatorname{ord}(\mathrm{loc}_\ell(\kappa^{(\ell)}), H^1(\mathbb{Q}_\ell, E)[q]) = \operatorname{ord}(\mathrm{loc}_\ell(\kappa), H^1(\mathbb{Q}_\ell, E[q])).$$

Hence, by Claim 2 (2), we have

$$\mathrm{loc}_\ell(\kappa^{(\ell)}) \notin H^1_f(\mathbb{Q}_\ell, E[q]).$$

Then, we obtain a contradiction to Claim 3, and hence complete the proof.

□

Remark 4.3.12. If the image of $\kappa^{(\ell)}$ in $H^1(\mathbb{Q}_p, E[q])$ always belonged to $E(\mathbb{Q}_p)/q$ as the class $d(\ell)$ in [8, Theorem 4.9], we were able to assume $\mathrm{ord}(D) < r_q(\mathrm{Sel}(\mathbb{Q}, E[q]))$ instead of $\mathrm{ord}(D) < r_q(H^1_{f,p}(\mathbb{Q}, E[q]))$.

We put $\mathfrak{r}_{\min} = \min_{n\geq 1}\left\{r_{p^n}\left(H^1_{f,p}(\mathbb{Q}, E[p^n])\right)\right\}$. As a consequence of Theorem 4.3.10, we have the following.

Corollary 4.3.13. *Let S be a square-free product of primes ℓ relatively prime to pN with the following condition: if $\ell \equiv 1 \mod p$, then $E(\mathbb{F}_\ell)[p]$ is cyclic. Then, we have*

$$\sum_{\sigma\in\Gamma_S} z_S^{\sigma^{-1}} \otimes \sigma \in H^1(\mathbb{Q}(S), T) \otimes I_S^{\min\{\mathfrak{r}_{\min}, p\}}.$$

Remark 4.3.14.

1. Since $E(\mathbb{Q}(S))[p] = 0$, the cohomology group $H^1(\mathbb{Q}(S), T)$ is $\mathbb{Z}_p$-free.
2. If $E(\mathbb{Q}_p)/p \cong \mathbb{Z}/p\mathbb{Z}$ (e.g. p is not anomalous), then by Lemma 4.3.3 and by the exact sequence

$$0 \to H^1_{f,p}(\mathbb{Q}, E[p^n]) \to \mathrm{Sel}(\mathbb{Q}, E[p^n]) \to E(\mathbb{Q}_p)/p^n \text{ for all } n \geq 1,$$

we have $\mathfrak{r}_{\min} \geq \mathrm{rank}(E(\mathbb{Q})) - 1$.

Proof. We may assume that $\mathfrak{r}_{\min} \geq 1$. We apply Lemma 4.1.8 for $H^1(\mathbb{Q}(S), T)$ and z_S. Let D be a derivative such that $\mathrm{Supp}(D) = S$ and $\mathrm{ord}(D) < \min\{\mathfrak{r}_{\min}, p\}$. We put $S' := \mathrm{Cond}(D)$. Then, we have

$$D = D' N_{\frac{S}{S'}}$$

for some derivative D' such that

$$\mathrm{Supp}(D') = \mathrm{Cond}(D') = S', \quad n(D') = n(D), \quad \mathrm{ord}(D') = \mathrm{ord}(D).$$

We have

$$Dz_S = \left(\prod_{v|(S/S')} P_v(\mathrm{Fr}_v^{-1})\right) D' z_{S'},$$

where v ranges over all the primes dividing S/S'.

We recall that $n(D)$ is defined as $\min_{\ell|\mathrm{Cond}(D)}\{|\Gamma_\ell|\}$ (cf. Definition 4.1.2). Thus, if we put $q = n(D')$, which is a power of p, then $S' \in \mathscr{N}_q$. Since

$$\mathrm{ord}(D') = \mathrm{ord}(D) < \mathfrak{r}_{\min} \leq r_q\left(H^1_{f,p}(\mathbb{Q}, E[q])\right), \quad \max_{\ell|S'}\{e_\ell(D')\} \leq \mathrm{ord}(D') < p,$$

Theorem 4.3.10 implies that

$$D' z_{S'} \equiv 0 \mod q,$$

and hence

$$Dz_S \equiv 0 \mod q.$$

Consequently, Lemma 4.1.8 shows that

$$\sum_{\sigma\in\Gamma_S} z_S^{\sigma^{-1}} \otimes \sigma - N_S z_S \otimes 1 \in H^1(\mathbb{Q}(S), T) \otimes I_S^{\min\{\mathfrak{r}_{\min}, p\}}.$$

Since $\mathfrak{r}_{\min} \geq 1$ and $H^1(\mathbb{Q}, E[p^n]) \to H^1(\mathbb{Q}, E[p^\infty])$ is injective for all $n \geq 1$, the cohomology group $H^1_{f,p}(\mathbb{Q}, E[p^\infty]) := \varinjlim H^1_{f,p}(\mathbb{Q}, E[p^n])$ is *not* finite. By [36, Theorem 2.2.3] (our $H^1_{f,p}(\mathbb{Q}, E[p^\infty])$ coincides with $\mathscr{S}_{\Sigma_p}(\mathbb{Q}, E[p^\infty])$ in [36]), we have $z_1 = 0$. Then, we have $N_S z_S = \prod_{\ell|S} P_\ell(\ell^{-1}) z_1 = 0$, and hence

$$\sum_{\sigma\in\Gamma_S} z_S^{\sigma^{-1}} \otimes \sigma \in H^1(\mathbb{Q}(S), T) \otimes I_S^{\min\{\mathfrak{r}_{\min}, p\}}.$$

□

4.3.3 A modification of the theorem

As stated before, we give a slight modification of Theorem 4.3.10.

Theorem 4.3.15. *Let q be a power of p. Let D be a Darmon-Kolyvagin derivative with support S satisfying $\max_{\ell|S}\{e_\ell(D)\} < p$. We suppose that $S \in \mathscr{N}_q$ and for each prime ℓ dividing S, $E(\mathbb{F}_\ell)[q]$ is isomorphic to $\mathbb{Z}/q\mathbb{Z}$ or 0. We put $S' = \mathrm{Cond}(D)$ and recall that $A_q(S') := \oplus_{\ell|S'} E(\mathbb{Q}_\ell)/q$. If $\mathrm{ord}(D) < r_q\left(H^1_{f,pS'}(\mathbb{Q}, E[q])\right) + r_p(A_q(S'))$, then we have*

$$Dz_S \equiv 0 \mod q.$$

Remark 4.3.16. By the exact sequence $0 \to H^1_{f,pS'} \to H^1_{f,p} \to \oplus_{\ell|S'} E(\mathbb{Q}_\ell)/q$ and Lemma 4.3.3, we have

$$r_q(H^1_{f,p}(\mathbb{Q}, E[q])) \leq r_q\left(H^1_{f,pS'}(\mathbb{Q}, E[q])\right) + r_p(A_q(S')).$$

In particular, when $q = p$, Theorem 4.3.15 implies Theorem 4.3.10

Lemma 4.3.17. *We fix $w \in \mathbb{Z}$, and assume that Theorem 4.3.15 holds for any derivative whose weight is strictly less than w. Let D, S, S' be as in Theorem 4.3.15. We suppose that $w(D) = w$. Then, the following assertions hold.*

1. *We have*

$$Dz_S \in H^0\left(\Gamma_S, H^1(\mathbb{Q}(S), T)/q\right).$$

2. *We take a prime $\ell \in \mathscr{R}_{E,q}$ such that ℓ splits completely in $\mathbb{Q}(S)$ and suppose that $E(\mathbb{F}_\ell)[q] \cong \mathbb{Z}/q\mathbb{Z}$. Then, we have*

$$DD_\ell^{(1)} z_{S\ell} \in H^0\left(\Gamma_{S\ell}, H^1(\mathbb{Q}(S\ell), T)/q\right).$$

PROOF. We simply write $H^1_{f,*} = H^1_{f,*}(\mathbb{Q}, E[q])$. We write $S = \ell_1 \cdots \ell_s$ and $D = D_{\ell_1}^{(k_1)} \cdots D_{\ell_s}^{(k_s)}$. Then, each ℓ_i satisfies one of the following conditions.

(i) $k_i = 0$.

(ii) $k_i \geq 2$.

(iii) $k_i = 1$, $\ell_i \in \mathscr{R}_q \setminus \mathscr{R}_{E,q}$, and hence $E(\mathbb{Q}_{\ell_i})/q = 0$.

(iv) $k_i = 1$, $\ell_i \in \mathscr{R}_{E,q}$, and hence $E(\mathbb{Q}_{\ell_i})/q \cong \mathbb{Z}/q\mathbb{Z}$.

We first prove the assertion 1. It suffices to show that

$$Dz_S \in H^0\left(\Gamma_{\ell_i}, H^1(\mathbb{Q}(S), T)/q\right)$$

for each $1 \leq i \leq s$.

We only need to consider the case $i = 1$. In the case $k_1 = 0$, we have $D \in N_\ell \mathbb{Z}[\Gamma_S]$, and hence $Dz_S \in H^0\left(\Gamma_{\ell_1}, H^1(\mathbb{Q}(S), T)/q\right)$.

Then, we may assume that $k_1 \geq 1$. By Lemma 4.1.1, we have

$$(\sigma_{\ell_1} - 1)D \equiv -\sigma_{\ell_1} D_{\ell_1}^{(k_1-1)} D_{\ell_2}^{(k_2)} \cdots D_{\ell_s}^{(k_s)} \mod q\mathbb{Z}[\Gamma_S]. \tag{4.3.18}$$

We put $D' = D_{\ell_1}^{(k_1-1)} D_{\ell_2}^{(k_2)} \cdots D_{\ell_s}^{(k_s)}$. Then

$$\mathrm{Supp}(D') = S, \quad \mathrm{ord}(D') = \mathrm{ord}(D) - 1,$$

and we have

$$w(D') = w(D) - 1.$$

It suffices to show that

$$D'z_S \equiv 0 \mod q.$$

We consider the cases (ii), (iii) or (iv).

Case (ii). In this case, we have $\mathrm{Cond}(D') = S'$. We recall that

$$\mathrm{ord}(D') < \mathrm{ord}(D) < r_q(H^1_{f,pS'}) + r_p(A_q(S')).$$

Then, Theorem 4.3.15 holds for D', that is, $D'z_S \equiv 0 \mod q$. Thus, we complete the case (ii).

Case (iii). We have

$$D' = N_{\ell_i} D'',$$

where D'' is a derivative satisfying

$$\mathrm{Supp}(D'') = S/\ell_i, \quad \mathrm{Cond}(D'') = S'/\ell_i, \quad \mathrm{ord}(D'') = \mathrm{ord}(D) - 1.$$

Then,

$$D' z_S \equiv N_{\ell_1} D'' z_S \equiv P_{\ell_1}(\mathrm{Fr}_{\ell_1}^{-1}) D'' z_{S/\ell_1} \mod q.$$

It suffices to show that $D'' z_{S/\ell_1} \equiv 0 \mod q$. Since $E(\mathbb{Q}_{\ell_1})/q = 0$, we have

$$r_q(H^1_{f,pS'/\ell_i}) = r_q(H^1_{f,pS'}), \quad r_p(A_q(S'/\ell_1)) = r_p(A_q(S')).$$

Then, we have

$$\mathrm{ord}(D'') < r_q(H^1_{f,pS'/\ell_1}) + r_p(A_q(S'/\ell_1)).$$

Since $\ell_1 \notin \mathscr{R}_{E,q}$, we have

$$\begin{aligned} w(D'') &= \mathrm{ord}(D'') - |\{\ell' \in \mathscr{R}_{E,q};\ \ell' \text{ divides } S/\ell_1\}| \\ &= \mathrm{ord}(D) - 1 - |\{\ell' \in \mathscr{R}_{E,q};\ \ell' \text{ divides } S\}| \\ &= w(D) - 1. \end{aligned}$$

Hence, Theorem 4.3.15 holds for D'', that is, $D'' z_{S/\ell_1} \equiv 0 \mod q$.

Case (iv). In this case, we have $\mathrm{Cond}(D') = S'/\ell_1$. By using Lemma 4.3.5, we obtain

$$\begin{aligned} \mathrm{ord}(D') = \mathrm{ord}(D) - 1 &< r_q(H^1_{f,pS'}) + r_p(A_q(S')) - 1 \\ &\leq r_q(H^1_{f,pS'/\ell_1}) + r_p(A_q(S'/\ell_1)). \end{aligned}$$

Then, Theorem 4.3.15 holds for D', that is, $D' z_{S/\ell_i} \equiv 0 \mod q$. Therefore, we prove the assertion 1 of the lemma.

Next, we prove the assertion 2 of the lemma.

The same calculation as (4.3.9) in the proof of Lemma 4.3.11 shows that

$$DD^{(1)}_\ell z_{S\ell} \in H^0\left(\Gamma_\ell, H^1(\mathbb{Q}(S\ell), T)/q\right). \tag{4.3.19}$$

The rest of the proof consists of two steps.

Step 1. For each ℓ_i satisfying the conditions (i), (ii) or (iii) above, we have

$$DD^{(1)}_\ell z_{S\ell} \in H^0\left(\Gamma_{\ell_i}, H^1(\mathbb{Q}(S\ell), T)/q\right).$$

It suffices to consider the case $i = 1$

Case (i). We easily have $DD^{(1)}_\ell z_{S\ell} \in H^0\left(\Gamma_{\ell_1}, H^1(\mathbb{Q}(S\ell), T)/q\right)$.

Case (ii). By Lemma 4.1.1, we have

$$(\sigma_{\ell_1} - 1)D \equiv -\sigma_{\ell_1} D_{\ell_1}^{(k_1-1)} D_{\ell_2}^{(k_2)} \cdots D_{\ell_s}^{(k_s)} \mod q\mathbb{Z}[\Gamma_S]. \tag{4.3.20}$$

If we put $D' = D_{\ell_1}^{(k_1-1)} D_{\ell_2}^{(k_2)} \cdots D_{\ell_s}^{(k_s)}$, then

$$\mathrm{Supp}(D') = S, \quad \mathrm{Cond}(D') = S', \quad \mathrm{ord}(D') = \mathrm{ord}(D) - 1.$$

By (4.3.4), we have

$$\mathrm{ord}(D) < r_q(H^1_{f,pS'}) + r_p(A(S')) \leq r_q(H^1_{f,pS'\ell}) + r_p(A(S'\ell)),$$

and hence by the equation $\mathrm{ord}(D'D_\ell^{(1)}) = \mathrm{ord}(D)$,

$$\mathrm{ord}(D'D_\ell^{(1)}) < r_q(H^1_{f,pS'\ell}) + r_p(A(S'\ell)).$$

Since $\mathrm{Supp}(D'D_\ell^{(1)}) = S\ell$, we have

$$\begin{aligned} w(D'D_\ell^{(1)}) &= \mathrm{ord}(D'D_\ell^{(1)}) - |\{\ell' \in \mathscr{R}_{E,q};\ \ell' \text{ divides } S\ell\}| \\ &= \mathrm{ord}(D) - |\{\ell' \in \mathscr{R}_{E,q};\ \ell' \text{ divides } S\}| - 1 \\ &= w(D) - 1. \end{aligned}$$

Then, Theorem 4.3.15 hods for $D'D_\ell^{(1)}$, that is,

$$D'D_\ell^{(1)} z_{S\ell} \equiv 0 \mod q.$$

By (4.3.20), we have $DD_\ell^1 z_{S\ell} \in H^0\left(\Gamma_{\ell_1}, H^1(\mathbb{Q}(S\ell), T)/q\right)$.

Case (iii). We have

$$(\sigma_{\ell_1} - 1)D \equiv -N_{\ell_1} D'',$$

where D'' is a derivative satisfying

$$\mathrm{Supp}(D'') = S/\ell_1, \quad \mathrm{Cond}(D'') = S'/\ell_1, \quad \mathrm{ord}(D'') = \mathrm{ord}(D) - 1.$$

Then, we have

$$(\sigma_{\ell_1} - 1)DD_\ell^{(1)} z_{S\ell} \equiv -N_{\ell_1} D''D_\ell^{(1)} z_{S\ell} \equiv -P_{\ell_1}(\mathrm{Fr}_{\ell_1}^{-1}) D''D_\ell^{(1)} z_{S\ell/\ell_1} \mod q.$$

Hence, it suffices to show that $D''D_\ell^{(1)} z_{S\ell/\ell_1} \equiv 0 \mod q$. Since $\ell_1 \notin \mathscr{R}_{E,q}$, we have

$$\begin{aligned} w(D''D_\ell^{(1)}) &= \mathrm{ord}(D''D_\ell^{(1)}) - |\{\ell' \in \mathscr{R}_{E,q};\ \ell' |\ \text{ divides } S\ell/\ell_1\}| \\ &= \mathrm{ord}(D) - |\{\ell' \in \mathscr{R}_{E,q};\ \ell' |\ \text{ divides } S\}| - 1 \\ &= w(D) - 1. \end{aligned}$$

In addition, since $E(\mathbb{Q}_{\ell_1})/q = 0$, we have

$$r_q(H^1_{f,pS'\ell/\ell_1}) = r_q(H^1_{f,pS'\ell}), \quad r_p(A_q(S'\ell/\ell_1)) = r_p(A_q(S'\ell)).$$

Then, Lemma 4.3.5 shows that

$$\mathrm{ord}(D) < r_q(H^1_{f,pS'}) + r_p(A_q(S')) \leq r_q(H^1_{f,pS'\ell/\ell_1}) + r_p(A_q(S'\ell/\ell_1)),$$

and hence

$$\mathrm{ord}(D''D^{(1)}_\ell) < r_q(H^1_{f,pS'\ell/\ell_1}) + r_p(A_q(S'\ell/\ell_1)).$$

Hence, Theorem 4.3.15 hods for $D''D^{(1)}_\ell$, that is, $D''D^{(1)}_\ell z_{S\ell/\ell_i} \equiv 0 \mod q$. Then, we complete Step 1.

Step 2. We prove the assertion 2 of the lemma by induction on the number n of primes satisfying (iv). Without loss of generality, we may write $S = \ell_1 \cdots \ell_s$, where $\ell_1, \ell_2, \ldots, \ell_n$ satisfy (iv) and $\ell_{n+1}, \ell_{n+2}, \ldots, \ell_s$ satisfy (i), (ii) or (iii).

The case $n = 0$. This case follows from Step 1 and (4.3.19).

The case $n \geq 1$. By Step 1 and (4.3.19), we are reduced to showing that

$$DD^{(1)}_\ell z_{S\ell} \in H^0\left(\Gamma_{\ell_i}, H^1(\mathbb{Q}(S\ell), T)/q\right)$$

for $1 \leq i \leq n$. It suffices to consider the case $i = 1$. Let $S_1 = S/\ell_1$ and $D_{S_1} = D^{k_2}_{\ell_2} \cdots D^{k_s}_{\ell_s}$. Then, we have $D = D^{(1)}_{\ell_1} D_{S_1}$ and

$$(\sigma_{\ell_1} - 1)DD^{(1)}_\ell z_{S\ell} \equiv -N_{\ell_1} D_{S_1} D^{(1)}_\ell z_{S\ell} \equiv -P_{\ell_1}(\mathrm{Fr}^{-1}_{\ell_1}) D_{S_1} D^{(1)}_\ell z_{S_1\ell} \mod q.$$

Since $\ell_1 \in \mathscr{R}_{E,q}$, if we prove that

$$D_{S_1} D^{(1)}_\ell z_{S_1\ell} \in H^0\left(\Gamma_{S_1\ell}, H^1(\mathbb{Q}(S_1\ell), T)/q\right), \tag{4.3.21}$$

then we have

$$P_{\ell_1}(\mathrm{Fr}^{-1}_{\ell_1}) D_{S_1} D^{(1)}_\ell z_{S_1\ell} \equiv P_{\ell_1}(1) D_{S_1} D^{(1)}_\ell z_{S_1\ell} \equiv 0 \mod q,$$

and complete Step 2. We prove (4.3.21). By Lemma 4.3.5,

$$\begin{aligned}\mathrm{ord}(D_{S_1}) = \mathrm{ord}(D) - 1 &< r_q(H^1_{f,pS'}) + r_p(A(S')) - 1 \\ &\leq r_q(H^1_{f,pS'/\ell_1}) + r_p(A(S'/\ell_1)).\end{aligned}$$

We recall that $\mathrm{Cond}(D_{S_1}) = S'/\ell_1$. Since $w(D_{S_1}) = w(D) = w$, we may apply the induction hypothesis on n to D_{S_1}, and the obtain (4.3.21). □

Proof of Theorem 4.3.15. As in the proof of Theorem 4.3.10, Theorem 4.3.15 is proved by induction on $w(D)$. Since $\mathrm{ord}(D) < r_q\left(H^1_{f,pS'}(\mathbb{Q}, E[q])\right) + r_p(A_q(S'))$, we have $r_q(H^1_{f,pS'}(\mathbb{Q}, E[q])) > 0$. By using Lemma 4.3.17 instead of Lemma 4.3.11, we complete the proof in the same way as that in the proof of Theorem 4.3.10 . □

Corollary 4.3.18. *Let q be a power of p. Let D be a Darmon-Kolyvagin derivative with support S satisfying $\max_{\ell|S}\{e_\ell(D)\} < p$. We suppose that $S \in \mathscr{N}_q$ and for each $\ell|S$, $E(\mathbb{F}_\ell)[q]$ is isomorphic to $\mathbb{Z}/q\mathbb{Z}$ or 0. We put $S' = \mathrm{Cond}(D)$. We assume that $\mathrm{ord}(D) \leq r_q\left(H^1_{f,pS'}(\mathbb{Q}, E[q])\right) + r_p(A_q(S'))$. Then*

$$Dz_S \in H^0\left(\Gamma_S, H^1(\mathbb{Q}(S), T)/q\right).$$

Proof. The proof is similar to that of Lemma 4.3.17.

We write $S = \ell_1 \cdots \ell_s$ and $D = D_{\ell_1}^{(k_1)} \cdots D_{\ell_s}^{(k_s)}$. Then, each ℓ_i satisfies one of the following conditions.

(i) $k_i = 0$.

(ii) $k_i \geq 2$.

(iii) $k_i = 1$, $\ell_i \in \mathscr{R}_q \setminus \mathscr{R}_{E,q}$, and hence $E(\mathbb{Q}_{\ell_i})/q = 0$.

(iv) $k_i = 1$, $\ell_i \in \mathscr{R}_{E,q}$, and hence $E(\mathbb{Q}_{\ell_i})/q \cong \mathbb{Z}/q\mathbb{Z}$.

Step A. For ℓ_i satisfying (i), (ii), or (iii), we have

$$Dz_S \in H^0\left(\Gamma_{\ell_i}, H^1(\mathbb{Q}(S), T)/q\right).$$

It suffices to consider the case $i = 1$.

Case (i). This case is trivial.

Case (ii). By Lemma 4.1.1, we have

$$(\sigma_{\ell_1} - 1)D \equiv -\sigma_{\ell_1} D_{\ell_1}^{(k_1-1)} D_{\ell_2}^{(k_2)} \cdots D_{\ell_s}^{(k_s)} \mod q\mathbb{Z}[\Gamma_S]. \tag{4.3.22}$$

Since $k_1 \geq 2$, if we put $D' = D_{\ell_1}^{(k_1-1)} D_{\ell_2}^{(k_2)} \cdots D_{\ell_s}^{(k_s)}$, then

$$\mathrm{Supp}(D') = S, \quad \mathrm{Cond}(D') = S', \quad \mathrm{ord}(D') = \mathrm{ord}(D) - 1.$$

By the assumption on $\mathrm{ord}(D)$,

$$\mathrm{ord}(D') < r_q(H^1_{f,pS'}) + r_p(A(S'))$$

Hence, by Theorem 4.3.15, we have $D'z_S \equiv 0 \mod q$, and then by (4.3.22), we complete the case (ii).

(iii). We have

$$(\sigma_{\ell_1} - 1)D \equiv -N_{\ell_1} D'',$$

where D'' is a derivative satisfying

$$\mathrm{Supp}(D'') = S/\ell_1, \quad \mathrm{Cond}(D'') = S'/\ell_1, \quad \mathrm{ord}(D'') = \mathrm{ord}(D) - 1.$$

Then, we have

$$(\sigma_{\ell_1} - 1)Dz_S \equiv -N_{\ell_1} D'' z_S \equiv -P_{\ell_1}(\mathrm{Fr}_{\ell_1}^{-1}) D'' z_{S/\ell_1} \mod q.$$

It suffices to show that $D'' z_{S/\ell_1} \equiv 0 \mod q$. By the equation $E(\mathbb{Q}_{\ell_1})/q = 0$, we have

$$r_q(H^1_{f,pS'/\ell_1}) = r_q(H^1_{f,pS'}), \quad r_p(A_q(S'/\ell_1)) = r_p(A_q(S')).$$

Hence, we have

$$\mathrm{ord}(D'') < r_q(H^1_{f,pS'/\ell_1}) + r_p(A_q(S'/\ell_1)),$$

Then, Theorem 4.3.15 implies that $D'' z_{S/\ell_1} \equiv 0 \mod q$, and we complete Step A.

Step B. We prove the corollary by induction on the number n of primes satisfying (iv). Without loss of generality, we may write $S = \ell_1 \cdots \ell_s$, where $\ell_1, \ell_2, \ldots, \ell_n$ satisfy (iv) and $\ell_{n+1}, \ell_{n+2}, \ldots, \ell_s$ satisfy (i), (ii) or (iii).

The case $n = 0$. This case is completed by Step A.

The case $n \geq 1$. By Step A, we are reduced to showing that

$$Dz_S \in H^0\left(\Gamma_{\ell_i}, H^1(\mathbb{Q}(S), T)/q\right)$$

for $1 \leq i \leq n$. It suffices to show this for ℓ_1. We put $S_1 = S/\ell_1$ and $D_{S_1} = D_{\ell_2}^{k_2} \cdots D_{\ell_s}^{k_s}$. Then, $D = D_{\ell_1}^{(1)} D_{S_1}$, and we have

$$(\sigma_{\ell_1} - 1)Dz_S \equiv -N_{\ell_1} D_{S_1} z_S \equiv -P_{\ell_1}(\mathrm{Fr}_{\ell_1}^{-1}) D_{S_1} z_{S_1} \mod q.$$

By Lemma 4.3.5, we have

$$\begin{aligned} \mathrm{ord}(D_{S_1}) = \mathrm{ord}(D) - 1 &\leq r_q(H^1_{f,pS'}) + r_p(A(S')) - 1 \\ &\leq r_q(H^1_{f,pS'/\ell_1}) + r_p(A(S'/\ell_1)). \end{aligned}$$

By the induction hypothesis, we have $D_{S_1} z_{S_1} \in H^0\left(\Gamma_{S_1}, H^1(\mathbb{Q}(S_1), T)/q\right)$, and hence $P_{\ell_1}(\mathrm{Fr}_{\ell_1}^{-1}) D_{S_1} z_{S_1} \equiv 0 \mod q$. □

4.4 Local behavior of derivatives of Euler systems at p

In this section, we study local conditions of derivatives of Euler systems at p. The aim of this section is to show that if certain localization of derivatives of Euler systems at p is not divided by p, then the order of the Tate-Shafarevich group is not divided by p. See Corollary 4.4.3 for the detail.

We keep the notation and assumption as in Section 4.3. We put $r_E = \mathrm{rank}(E(\mathbb{Q}))$, and denote by Ш the Tate-Shafarevich group of E over $\mathbb{Q}$.

Assumption 4.4.1. We assume that $E(\mathbb{Q}_p)/p \cong \mathbb{Z}/p\mathbb{Z}$, or equivalently, $E(\mathbb{Q}_p)[p] = 0$ (cf. (2.1.3)).

We note that if $p \nmid |E(\mathbb{F}_p)|$, then Assumption 4.4.1 holds. By Lemma 4.3.3, Assumption 4.4.1 implies that $r_p(H^1_{f,p}(\mathbb{Q}, E[p])) \geq r_p(\mathrm{Sel}(\mathbb{Q}, E[p])) - 1 \geq r_E - 1$.

For a positive integer S and $A = T_p(E), V_p(E)$ or $E[p]$, we put

$$H^1(\mathbb{Q}(S) \otimes \mathbb{Q}_p, A) = \oplus_{\lambda|p} H^1(\mathbb{Q}(S)_\lambda, A),$$

where λ ranges over all the primes of $\mathbb{Q}(S)$ dividing p, and $\mathbb{Q}(S)_\lambda$ denotes the completion at λ. We denote by $H^1_f(\mathbb{Q}(S) \otimes \mathbb{Q}_p, A)$ the image of the Kummer map, and define

$$H^1_{/f}(\mathbb{Q}(S) \otimes \mathbb{Q}_p, A) = \frac{H^1(\mathbb{Q}(S) \otimes \mathbb{Q}_p, A)}{H^1_f(\mathbb{Q}(S) \otimes \mathbb{Q}_p, A)}.$$

For $\eta \in H^1(\mathbb{Q}(S), E[p])$, we denote by $\mathrm{loc}_p(\eta)$ the image of η in $H^1(\mathbb{Q}(S) \otimes \mathbb{Q}_p, E[p])$.

Theorem 4.4.2. *We assume that $E(\mathbb{Q}_p)/p \cong \mathbb{Z}/p\mathbb{Z}$. Let D be a Darmon-Kolyvagin derivative with support S such that $\max_{\ell|S}\{e_\ell(D)\} < p$. We suppose that $S \in \mathscr{N}_p$ and for each prime ℓ dividing S, $E(\mathbb{F}_\ell)[p]$ is cyclic (i.e. $E(\mathbb{F}_\ell)[p]$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or 0). We put $S' = \mathrm{Cond}(D)$. If $\mathrm{ord}(D) < r_p\left(H^1_{f,S'}(\mathbb{Q}, E[p])\right) + r_p(A_p(S'))$, then the following assertions hold.*

1. *$Dz_S \in H^0\left(\Gamma_S, H^1(\mathbb{Q}(S), T)/p\right)$.*
2. *If we denote by κ the inverse image of $Dz_S \in H^1(\mathbb{Q}(S), E[p])$ under the isomorphism $H^1(\mathbb{Q}, E[p]) \cong H^0\left(\Gamma_S, H^1(\mathbb{Q}(S), E[p])\right)$, then we have*

$$\mathrm{loc}_p(\kappa) \in H^1_f(\mathbb{Q}_p, E[p]).$$

Proof. We simply write $H^1_{f,*} = H^1_{f,*}(\mathbb{Q}, E[p])$. By the exact sequence

$$0 \to H^1_{f,pS'} \to H^1_{f,S'} \to E(\mathbb{Q}_p)/p, \tag{4.4.1}$$

we have

$$r_p\left(H^1_{f,S'}\right) \leq r_p\left(H^1_{f,pS'}\right) + 1.$$

Then, the assertion 1 follows from Corollary 4.3.18.

We prove the assertion 2. If $r_p\left(H^1_{f,S'}\right) = r_p\left(H^1_{f,pS'}\right)$, then by Theorem 4.3.15, we have $Dz_S \equiv 0 \mod pH^1(\mathbb{Q}(S), T)$, and hence $\kappa = 0$.

We assume that $r_p\left(H^1_{f,S'}\right) = r_p\left(H^1_{f,pS'}\right) + 1$. Then, by (4.4.1), the localization map $H^1_{f,S'} \to E(\mathbb{Q}_p)/p$ is surjective.

We recall that the pairing induced by the cup product

$$(-,-)_p : E(\mathbb{Q}_p)/p \times H^1_{/f}(\mathbb{Q}_p, E[p]) \to \mathbb{Z}/p\mathbb{Z}$$

is perfect. It then suffices to show that

$$(c,\kappa)_p = 0 \quad \text{for each } c \in E(\mathbb{Q}_p)/p.$$

We take an element c of $E(\mathbb{Q}_p)/p$. Since $H^1_{f,S'} \to E(\mathbb{Q}_p)/p$ is surjective, there exists an element $\eta \in H^1_{f,S'}$ whose localization at p coincides with c. Then, by the Hasse principle,

$$(c,\kappa)_p = (\eta,\kappa)_p = -\sum_{w\nmid p:\text{prime}} (\eta,\kappa)_w.$$

By the definition of $H^1_{f,S'}(\mathbb{Q}, E[p])$ and Corollary 4.2.11 for κ, we have $(\eta,\kappa)_w = 0$ for $w \nmid p$. Hence, we conclude that $(c,\kappa)_p = 0$. □

The following plays an important role in the proof of Theorem 5.4.2.

Corollary 4.4.3. *Let D be a Darmon-Kolyvagin derivative with support S. We suppose that $S \in \mathscr{N}_p$ and $E(\mathbb{F}_\ell)[p]$ is cyclic for each prime $\ell|S$. We assume that $p \geq r_E$ and $\mathrm{ord}(D) = r_E$. If $\mathrm{loc}_p(Dz_S) \notin H^1_f(\mathbb{Q}(S)\otimes\mathbb{Q}_p, E[p])$, then we have*

1. *$Ш[p] = 0$,*
2. *$E(\mathbb{Q})/p \to \oplus_{\ell|S} E(\mathbb{Q}_\ell)/p$ is surjective.*

Proof. We put $S' = \mathrm{Cond}(D)$. Since $\mathrm{loc}_p(Dz_S) \notin H^1_f(\mathbb{Q}(S)\otimes\mathbb{Q}_p, E[p])$, Theorem 4.4.2 implies that

$$r_E \geq r_p(H^1_{f,S'}) + r_p(A(S')).$$

On the other hand, by Lemma 4.3.3,

$$r_p(H^1_{f,S'}) + r_p(A(S')) \geq r_p(\mathrm{Sel}(\mathbb{Q}, E[p])).$$

Since $r_E \leq r_p(\mathrm{Sel}(\mathbb{Q}, E[q]))$, we have

$$r_E = r_p(H^1_{f,S'}) + r_p(A(S')) = r_p(\mathrm{Sel}(\mathbb{Q}, E[p])). \tag{4.4.2}$$

This implies that $Ш[p] = 0$, and the following sequence

$$0 \to H^1_{f,S'} \to E(\mathbb{Q})/p \to \oplus_{\ell|S'} E(\mathbb{Q}_\ell)/p \to 0$$

is exact. For the assertion 2, it suffices to show that $E(\mathbb{Q}_\ell)/p = 0$ for each prime ℓ dividing S/S'.

We assume that $E(\mathbb{Q}_\ell)/p \cong \mathbb{Z}/p\mathbb{Z}$ for some ℓ dividing S/S'. In particular, $\ell \in \mathscr{R}_{E,p}$. Since $\ell \nmid S'$, we have $D = N_\ell D'$ for some derivative D' such that $\mathrm{Supp}(D') = S/\ell$ and $\mathrm{ord}(D') = r_E$. We claim that

$$\mathrm{loc}_p(D' z_{S/\ell}) \in H^0(\Gamma_{S/\ell}, H^1_{/f}(\mathbb{Q}(S/\ell) \otimes \mathbb{Q}_p, E[p])). \tag{4.4.3}$$

To prove this, we take a prime ℓ' dividing S/ℓ. If $e_{\ell'}(D') = 0$, then $D' \in N_{\ell'}\mathbb{Z}[\Gamma_{S/\ell}]$, and hence $D' z_{S/\ell} \in H^0(\Gamma_{\ell'}, H^1_{/f}(\mathbb{Q}(S/\ell) \otimes \mathbb{Q}_p, E[p]))$. We assume that $e_{\ell'}(D') \geq 1$. Then, we have $(\sigma_{\ell'} - 1)D' \equiv -\sigma_{\ell'} D''$ mod p for some derivative D'' such that $\mathrm{ord}(D'') = r_E - 1$. If we put $S'' = \mathrm{Cond}(D'')$, then by Lemma 4.3.3, we have

$$r_E - 1 < r_p(\mathrm{Sel}(\mathbb{Q}, E[p])) \leq r_p(H^1_{f,S''}) + r_p(A_p(S'')).$$

Hence, by applying Theorem 4.4.2, we have

$$\log_p(D'' z_{S/\ell}) \in H^1_f(\mathbb{Q}(S/\ell) \otimes \mathbb{Q}_p, E[p]),$$

which implies that $\mathrm{loc}_p(D' z_{S/\ell}) \in H^0(\Gamma_{\ell'}, H^1_{/f}(\mathbb{Q}(S/\ell) \otimes \mathbb{Q}_p, E[p]))$. Then, we obtain (4.4.3). Hence, in $H^1_{/f}(\mathbb{Q}(S) \otimes \mathbb{Q}_p, E[p]))$,

$$\mathrm{loc}_p(D z_S) = \mathrm{loc}_p(N_\ell D' z_S) = P_\ell(\mathrm{Fr}_\ell^{-1})\mathrm{loc}_p(D' z_{S/\ell}) = P_\ell(1)\mathrm{loc}_p(D' z_{S/\ell}) = 0.$$

Then, we obtain a contradiction. □

4.5 Rational points from derivatives of Euler systems

In this section, we prove Theorem 4.5.2. We keep the notation and assumption as in Section 4.4.

Assumption 4.5.1. We assume that the natural map $E(\mathbb{Q})/p \to E(\mathbb{Q}_p)/p$ is surjective.

In particular, the localization map $\mathrm{Sel}(\mathbb{Q}, E[p]) \to E(\mathbb{Q}_p)/p$ is surjective, and hence by Assumption 4.4.1,

$$r_p\left(H^1_{f,p}(\mathbb{Q}, E[p])\right) = r_p\left(\mathrm{Sel}(\mathbb{Q}, E[p])\right) - 1.$$

We define a subgroup C_p of $E(\mathbb{Q})/p$ by

$$C_p = \ker\left(E(\mathbb{Q})/p \to E(\mathbb{Q}_p)/p\right).$$

Then, by Assumption 4.5.1, we have

$$r_p(C_p) = r_E - 1. \tag{4.5.1}$$

By applying the snake lemma to the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q})/p & \longrightarrow & \mathrm{Sel}(\mathbb{Q}, E[p]) & \longrightarrow & Ш[p] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(\mathbb{Q}_p)/p & \longrightarrow & E(\mathbb{Q}_p)/p & \longrightarrow & 0 & \longrightarrow & 0, \end{array}$$

we have an exact sequence

$$0 \to C_p \to H^1_{f,p}(\mathbb{Q}, E[p]) \to Ш[p] \to 0. \tag{4.5.2}$$

Now, we prove the following theorem.

Theorem 4.5.2. *We assume that the natural map $E(\mathbb{Q})/p \to E(\mathbb{Q}_p)/p$ is surjective and $E(\mathbb{Q}_p)/p \cong \mathbb{Z}/p\mathbb{Z}$. Let D be a Darmon-Kolyvagin derivative with support S such that $\max_{\ell|S}\{e_\ell(D)\} < p$. We suppose that $S \in \mathcal{N}_p$ and for each prime $\ell|S$, $E(\mathbb{F}_\ell)[p]$ is cyclic. We assume that $\mathrm{ord}(D) = r_E - 1$ and $Dz_S \not\equiv 0 \mod pH^1(\mathbb{Q}(S), T)$. Then, the following assertions hold.*

1. *$Ш[p] = 0$.*
2. *The localization map $H^1_{f,p}(\mathbb{Q}, E[p]) \to \oplus_{\ell|S} E(\mathbb{Q}_\ell)/p$ is surjective.*
3. *$Dz_S \in H^0\left(\Gamma_S, H^1(\mathbb{Q}(S), T)/p\right)$.*
4. *Let $\kappa \in H^1(\mathbb{Q}, E[p])$ be the inverse image of Dz_S under the isomorphism*

$$H^1(\mathbb{Q}, E[p]) \cong H^0\left(\Gamma_S, H^1(\mathbb{Q}(S), E[p])\right).$$

Then, we have

$$\kappa \in E(\mathbb{Q})/p.$$

Proof. 1. We simply write $H^1_{f,*} = H^1_{f,*}(\mathbb{Q}, E[p])$. Since $Dz_S \not\equiv 0 \mod p$, Theorem 4.3.10 implies that

$$r_E - 1 \geq r_p(H^1_{f,p}).$$

Hence, by (4.5.1) and (4.5.2), we have $r_p(H^1_{f,p}) = r_E - 1$ and $Ш[p] = 0$.

2. Since $\mathrm{ord}(D) = r_p(H^1_{f,p})$ and $Dz_S \not\equiv 0 \mod p$, Theorem 4.3.15 implies that

$$r_p(H^1_{f,p}) \geq r_p(H^1_{f,pS'}) + r_p(A_p(S')).$$

Therefore by Lemma 4.3.3, we have $r_p(H^1_{f,p}) = r_p(H^1_{f,pS'}) + r_p(A_p(S'))$. Then, the sequence

$$0 \to H^1_{f,pS'} \to H^1_{f,p} \to \oplus_{\ell|S'} E(\mathbb{Q}_\ell)/p \to 0 \tag{4.5.3}$$

is exact. In order to deduce the assertion 2, it suffices to show that $E(\mathbb{Q}_\ell)/p = 0$ for each prime ℓ dividing S/S'. We assume that $E(\mathbb{Q}_\ell)/p \cong \mathbb{Z}/p\mathbb{Z}$ for some prime ℓ dividing S/S'. In particular, $\ell \in \mathscr{R}_{E,p}$. Since $\ell \nmid S'$, we have

$$D = N_\ell D',$$

where D' is a derivative such that

$$\mathrm{Supp}(D') = S/\ell, \quad \mathrm{Cond}(D') = \mathrm{Cond}(D), \quad \mathrm{ord}(D') = \mathrm{ord}(D) = r_E - 1.$$

Corollary 4.3.18 implies that

$$D' z_{S/\ell} \in H^0\left(\Gamma_{S/\ell}, H^1(\mathbb{Q}(S/\ell), T)/p\right).$$

Hence, we have

$$D z_S = N_\ell D' z_S = P_\ell(\mathrm{Fr}_\ell^{-1}) D' z_{S/\ell} \equiv P_\ell(1) D' z_{S/\ell} \equiv 0 \mod p,$$

where the last equality follows from $\ell \in \mathscr{R}_{E,p}$. Hence, we obtain a contradiction, and deduce the assertion 2.

3. By Lemma 4.3.3, if we put $S' = \mathrm{Cond}(D')$, then we have

$$r_p(H^1_{f,p}) \leq r_p(H^1_{f,pS'}) + r_p(A_p(S')).$$

Since $r_E - 1 = r_p(H^1_{f,p})$, by Corollary 4.3.18, we deduce the assertion 3 of the theorem.

4. Since $Ш[p] = 0$, it suffices to show that $\kappa \in \mathrm{Sel}(\mathbb{Q}, E[p])$. By Corollary 4.2.11, we are reduced to showing that $\kappa \in E(\mathbb{Q}_\ell)/p$ for each prime $\ell | pS'$. By taking the Pontryagin dual of the sequence (4.5.3), the map

$$\varphi : \bigoplus_{\ell | S'} H^1(\mathbb{Q}_\ell, E)[p] \to H^1_{f,p}(\mathbb{Q}, E[p])^\vee; \ (g_\ell)_\ell \mapsto \left(\eta \mapsto \sum_{\ell | S'} (g_\ell, \eta)_\ell \right)$$

is injective. We first prove that the image of κ in $H^1(\mathbb{Q}_\ell, E)[p]$ is in the kernel of the map above. We take an element $\eta \in H^1_{f,p}(\mathbb{Q}, E[p])$. By the Hasse principle, we have

$$\sum_{\ell | S'} (\kappa, \eta)_\ell = -\sum_{v \nmid S'} (\kappa, \eta)_v = -(\kappa, \eta)_p = 0,$$

where the second equality follows from Corollary 4.2.11, and the last equality follows from the definition of $H^1_{f,p}(\mathbb{Q}, E[p])$. Since η is arbitrary, we have $\mathrm{loc}_\ell(\kappa) \in \ker(\varphi)$. Since the map φ is injective, we have $\mathrm{loc}_\ell(\kappa) \in E(\mathbb{Q}_\ell)/p$ for all $\ell | S'$. By Theorem 4.4.2, we also have

$$\mathrm{loc}_p(\kappa) \in E(\mathbb{Q}_p)/p.$$

Then, we deduce that $\kappa \in \mathrm{Sel}(\mathbb{Q}, E[p])$, and hence $\kappa \in E(\mathbb{Q})/p$. □

Chapter 5

Proof of the main result

In this chapter, we prove our main result on the Mazur-Tate refined conjecture of BSD type.

Throughout this chapter, we denote by E an elliptic curve over $\mathbb{Q}$ of conductor N without complex multiplication. We fix a global minimal Weierstrass model of E over $\mathbb{Z}$, and denote by ω the Néron differential. We also denote by Ω^+, Ω^- the periods as in Section 3.2. For a positive integer S, we put $G_S = \mathrm{Gal}(\mathbb{Q}(\mu_S)/\mathbb{Q})$.

5.1 Preliminaries on group rings

5.1.1 Local property

For this subsection, let p be a prime. For a finite abelian group G, we denote by I_G the augmentation ideal of $\mathbb{Z}_p[G]$.

Lemma 5.1.1. *For an element $\sigma \in G$ whose order is relatively prime to p, we have $\sigma - 1 \in I_G^t$ for all $t \geq 1$. In particular, if $p \nmid |G|$, then $I_G = I_G^2 = I_G^3 = \cdots$.*

Proof. We denote by n the order of σ. Then, we have

$$\begin{aligned} 0 = \sigma^n - 1 = (\sigma - 1 + 1)^n - 1 &= \sum_{k=1}^{n} \binom{n}{k} (\sigma - 1)^k \\ &= n(\sigma - 1) + \sum_{k=2}^{n} \binom{n}{k} (\sigma - 1)^k, \end{aligned}$$

and hence

$$n(\sigma - 1) = -(\sigma - 1)^2 \sum_{k=2}^{n} \binom{n}{k} (\sigma - 1)^{k-2} \in I_G^2. \tag{5.1.1}$$

Since $p \nmid n$, we see that $\sigma - 1 \in I_G^2$. Then, by using (5.1.1) again, we have $\sigma - 1 \in I_G^4$. By using (5.1.1) repeatedly, we conclude that $\sigma - 1 \in I_G^t$ for all $t \geq 1$. □

Lemma 5.1.2. *Suppose that we are given a decomposition $G = K \times H$ with $p \nmid |H|$. Let α be an element of $\mathbb{Z}_p[G]$. Let α_K denote the image of α under the map $\mathbb{Z}_p[G] \to \mathbb{Z}_p[K]$ induced by the projection $G \twoheadrightarrow K$. If $\alpha_K \in I_K^t$ for some $t \geq 1$, then $\alpha \in I_G^t$.*

PROOF. By the natural inclusion $\mathbb{Z}_p[K] \hookrightarrow \mathbb{Z}_p[G]$, we regard α_K as an element of $\mathbb{Z}_p[G]$. Then, we have

$$\alpha - \alpha_K \in \ker(\mathbb{Z}_p[G] \twoheadrightarrow \mathbb{Z}_p[K]) = \mathbb{Z}_p[K] \otimes_{\mathbb{Z}_p} I_H.$$

Lemma 5.1.1 implies that $\mathbb{Z}_p[K] \otimes I_H = \mathbb{Z}_p[K] \otimes I_H^t$. Since $\alpha_K \in I_K^t$, we have $\alpha \in I_G^t$. □

Lemma 5.1.3. *Under the notation as in Lemma 5.1.2, we suppose that $\alpha \in \mathbb{Z}_p \otimes I_G^t$. We denote by $\widetilde{\alpha}^{(p)}$ (resp. $\widetilde{\alpha}_K^{(p)}$) the image of α (resp. α_K) in $\mathbb{Z}/p\mathbb{Z} \otimes I_G^t/I_G^{t+1}$ (resp. $\mathbb{Z}/p\mathbb{Z} \otimes I_K^t/I_K^{t+1}$). If $\widetilde{\alpha}_K^{(p)} = 0$, then $\widetilde{\alpha}^{(p)} = 0$.*

PROOF. As in the poof of Lemma 5.1.2, we have

$$\alpha - \alpha_K \in \mathbb{Z}_p[K] \otimes I_H^t = \mathbb{Z}_p[K] \otimes I_H^{t+1} \subseteq \mathbb{Z}_p \otimes I_G^{t+1}.$$

Then, we have $\widetilde{\alpha} - \widetilde{\alpha}_K^{(p)} = 0$ in $\mathbb{Z}/p\mathbb{Z} \otimes I_G^t/I_G^{t+1}$, where we regard $\widetilde{\alpha}_K^{(p)}$ as an element of $\mathbb{Z}/p\mathbb{Z} \otimes I_G^t/I_G^{t+1}$ under the map induced by the inclusion $K \subseteq G$. Since $\widetilde{\alpha}_K^{(p)} = 0$, we have $\widetilde{\alpha}^{(p)} = 0$. □

5.1.2 Global property

Next, we fix a proper subring R of $\mathbb{Q}$, and we denote by I_G the augmentation ideal of $R[G]$.

Lemma 5.1.4. *Let α be an element of $R[G]$. For a positive integer t, the following conditions are equivalent*:

1. $\alpha \in I_G^t$,
2. $\alpha \in \mathbb{Z}_p \otimes_R I_G^t$ *for all the primes p not invertible in R.*

PROOF. We only need to show that the condition 2 implies the condition 1. It is proved by induction on t. First, we assume that $t = 1$. Then there exists a prime p such that $\alpha \in \mathbb{Z}_p \otimes I_G$. We note that we have the natural inclusion $R \hookrightarrow \mathbb{Z}_p$. Since $R[G]/I_G = R$ and $\mathbb{Z}_p[G]/(\mathbb{Z}_p \otimes_R I_G) = \mathbb{Z}_p$, we have $R/I_G \hookrightarrow \mathbb{Z}_p[G]/(\mathbb{Z}_p \otimes_R I_G)$. Hence, by the assumption 2, we have $\alpha \in I_G$.

We next assume that $t \geq 2$. By the condition 2 and the induction hypothesis, we have $\alpha \in I_G^{t-1}$. Combining Lemma 5.1.1 and the condition 2, the image of α in $\mathbb{Z}_p \otimes_R I_G^{t-1}/I_G^t$ is trivial for any prime p. Hence, the image of α in I_G^{t-1}/I_G^t is also trivial. □

5.2 Local study of Mazur-Tate elements

In this section, with a modification of ideas of [19], [21] and [33], we construct local points c_S of E, and relate (modified) Kato's Euler system to Mazur-Tate elements. Then, we apply results in Chapter 4 to obtain our main result.

Throughout this section, we fix a prime p such that

1. $p \nmid 6N \cdot |E(\mathbb{F}_p)| \prod_{\ell|N} m_\ell$,
2. the Galois representation $G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E))$ is surjective,

For a positive integer S, as in Chapter 4, we denote by $\mathbb{Q}(S)$ the maximal p-extension of $\mathbb{Q}$ inside $\mathbb{Q}(\mu_S)$ and put $\Gamma_S = \mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q})$. Let $\mathscr{O}_S$ denote the ring of integers of $\mathbb{Q}(S)$. We also put $H_S = \mathrm{Gal}(\mathbb{Q}(\mu_S)/\mathbb{Q}(S))$. Then, we have the canonical decomposition $G_S = H_S \times \Gamma_S$.

5.2.1 Construction of local points

For a finite unramified extension K of $\mathbb{Q}_p$ and its ring $\mathscr{O}$ of integers, we let σ denote the arithmetic Frobenius automorphism.

We denote by $\hat{E}$ the formal group law of E over $\mathbb{Z}_p$ (associated to ω) and by $\log_{\hat{E}}$ the logarithm of $\hat{E}$, which induces an isomorphism $\hat{E}(\mathscr{O}) \to p\mathscr{O}$.

Lemma 5.2.1. *We suppose that K is a finite unramified p-extension of $\mathbb{Q}_p$. Then, the homomorphism of $\mathbb{Z}_p$-modules defined as*

$$\hat{E}(\mathscr{O}) \to \mathscr{O};\ c \mapsto \left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right) \log_{\hat{E}}(c)$$

is an isomorphism, where $a_p = a_p(E)$ is as in Definition 2.2.1.

Proof. Since $\log_{\hat{E}} : \hat{E}(\mathscr{O}) \to p\mathscr{O}$ is an isomorphism, it suffices to show that the map $\left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right) : p\mathscr{O} \to \mathscr{O}$ is also an isomorphism. We put $d = [K : \mathbb{Q}_p]$, which is assumed to be a power of p.

We first assume that p is a good ordinary prime of E, that is, $p \nmid a_p$. Let $\alpha \in \mathbb{Z}_p^\times$ be the unit root of $X^2 - a_p X + p$ and $\beta \in p\mathbb{Z}_p$ the other root. Then we have

$$\left(1 - \frac{\sigma}{\alpha}\right)\left(1 - \frac{\sigma}{\beta}\right) = \left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right). \tag{5.2.1}$$

Since $p \nmid |E(\mathbb{F}_p)|$, we have $a_p \not\equiv 1 \mod p$, and hence $\alpha \not\equiv 1 \mod p$. Since d is a power of p, we obtain

$$\alpha^d - 1 \in \mathbb{Z}_p^\times. \tag{5.2.2}$$

For $A \in \mathscr{O}$, we put

$$x_A = \frac{\alpha^d}{\alpha^d - 1} \left(\sum_{0 \leq b \leq d-1} \frac{A^{\sigma^b}}{\alpha^b} \right) \in \mathscr{O},$$

then

$$\left(1 - \frac{\sigma}{\alpha}\right) x_A = A.$$

Since $\beta \in p\mathbb{Z}_p$,

$$y_A := -\sum_{k \geq 1} \beta^k x_A^{\sigma^{-k}} \in p\mathscr{O}$$

converges and satisfies

$$\left(1 - \frac{\sigma}{\beta}\right) y_A = x_A.$$

By (5.2.1), we have

$$\left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right) y_A = A.$$

Hence, we deduce that the map $\left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right) : p\mathscr{O} \to \mathscr{O}$ is surjective, and then it is an isomorphism.

We next assume that p is a good supersingular prime of E. Since $p \geq 5$, we have $a_p = 0$. For $A \in \mathscr{O}$, if we put $y_A = \sum_{k \geq 1} p^k A^{\sigma^{-2k}}$, then

$$(1 - \sigma^2/p) y_A = A.$$

Hence, the map $\left(1 + \frac{1}{p}\sigma^2\right) : p\mathscr{O} \to \mathscr{O}$ is surjective, and then it is an isomorphism. □

For each integer S relatively prime to p, we have $\mathscr{O}_S \otimes \mathbb{Z}_p = \prod_{\lambda | p} \mathscr{O}_{S,\lambda}$, where λ ranges over all the primes of $\mathbb{Q}(S)$ dividing p, and we denote by $\mathscr{O}_{S,\lambda}$ the completion of $\mathscr{O}_S$ at λ. Then, the logarithm $\log_{\hat{E}}$ naturally induces an isomorphism $\hat{E}(\mathscr{O}_S \otimes \mathbb{Z}_p) \to p\mathscr{O}_S \otimes \mathbb{Z}_p$, where $\hat{E}(\mathscr{O}_S \otimes \mathbb{Z}_p) := \oplus_{\lambda | p} \hat{E}(\mathscr{O}_{S,\lambda})$.

We recall that ζ_S denotes $\exp(2\pi i/S)$.

Definition 5.2.2. For a square-free product S of primes relatively prime to p, we define an element $c_S \in \hat{E}\left(\mathscr{O}_S \otimes \mathbb{Z}_p\right)$ by

$$\left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right) \log_{\hat{E}}(c_S) = \mathrm{tr}_{\mathbb{Q}(\mu_S)/\mathbb{Q}(S)}\left(\zeta_S\right) \in \mathscr{O}_S \otimes \mathbb{Z}_p. \tag{5.2.3}$$

By Lemma 5.2.1, the element c_S is well-defined.

We state basic properties of $\{c_S\}_S$, where S ranges over all square free products of primes relatively prime to p.

Proposition 5.2.3. *Let ℓ be a prime not dividing pS. Then, we have*

$$\mathrm{Tr}_{S\ell/S}(c_{S\ell}) = -c_S^{\mathrm{Fr}_\ell^{-1}},$$

where $\mathrm{Tr}_{S\ell/S} : \hat{E}(\mathscr{O}_{S\ell} \otimes \mathbb{Z}_p) \to \hat{E}(\mathscr{O}_S \otimes \mathbb{Z}_p)$ is the trace map with respect to the addition of $\hat{E}$.

Proof. By Lemma 5.2.1, it suffices to show that

$$\mathrm{tr}_{\mathbb{Q}(S\ell)/\mathbb{Q}(S)} \circ \mathrm{tr}_{\mathbb{Q}(\mu_{S\ell})/\mathbb{Q}(S\ell)} (\zeta_{S\ell}) = -\mathrm{tr}_{\mathbb{Q}(\mu_S)/\mathbb{Q}(S)} \left(\zeta_S^{\mathrm{Fr}_\ell^{-1}}\right).$$

Since

$$\mathrm{tr}_{\mathbb{Q}(S\ell)/\mathbb{Q}(S)} \circ \mathrm{tr}_{\mathbb{Q}(\mu_{S\ell})/\mathbb{Q}(S\ell)} = \mathrm{tr}_{\mathbb{Q}(\mu_S)/\mathbb{Q}(S)} \circ \mathrm{tr}_{\mathbb{Q}(\mu_{S\ell})/\mathbb{Q}(\mu_S)},$$

we are reduced to showing that $\mathrm{tr}_{\mathbb{Q}(\mu_{S\ell})/\mathbb{Q}(\mu_S)}(\zeta_{S\ell}) = -\zeta_S^{\mathrm{Fr}_\ell^{-1}}$. We put $\alpha = \zeta_S^{\mathrm{Fr}_\ell^{-1}}$. Then,

$$X^\ell - \zeta_S = X^\ell - \alpha^\ell = (X-\alpha)(X^{\ell-1} + \alpha X^{\ell-2} + \cdots + \alpha^{\ell-2}X + \alpha^{\ell-1}) \text{ in } \mathbb{Q}(\mu_S)[X].$$

Since $X^{\ell-1} + \alpha X^{\ell-2} + \cdots + \alpha^{\ell-2}X + \alpha^{\ell-1}$ is irreducible over $\mathbb{Q}(\mu_S)$ and $\zeta_{S\ell}$ is a root of the polynomial, we have $\mathrm{tr}_{\mathbb{Q}(\mu_{S\ell})/\mathbb{Q}(\mu_S)}(\zeta_{S\ell}) = -\alpha$. □

Proposition 5.2.4. *Let χ be a character of Γ_S. Then, we have*

$$\left(1 - \frac{a_p}{p}\chi(p)^{-1} + \frac{1}{p}\chi(p)^{-2}\right) \sum_{\delta \in \Gamma_S} \log_{\hat{E}}(c_S^\delta)\chi(\delta) = \tau_S(\chi).$$

On the right hand side, we regard χ as a character of $G_S = \Gamma_S \times H_S$ by $\chi|_{H_S} = 1$, and recall that $\tau_S(\chi) := \sum_{\gamma \in G_S} \chi(\gamma)\zeta_S^\gamma$.

Proof. By (5.2.3), we have

$$\begin{aligned} \sum_{\delta \in \Gamma_S} \delta \left(\left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right) \log_{\hat{E}}(c_S)\right) \chi(\delta) &= \sum_{\delta \in \Gamma_S} \delta \left(\mathrm{tr}_{\mathbb{Q}(\mu_S)/\mathbb{Q}(S)}(\zeta_S)\right) \chi(\delta) \\ &= \sum_{\gamma \in G_S} \zeta_S^\gamma \chi(\gamma) = \tau_S(\chi). \end{aligned} \tag{5.2.4}$$

On the other hand, we have

$$\begin{aligned} &\sum_{\delta \in \Gamma_S} \delta \left(\left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right) \log_{\hat{E}}(c_S)\right) \chi(\delta) \\ &= \sum_{\delta \in \Gamma_S} \left(1 - \frac{a_p}{p}\sigma + \frac{1}{p}\sigma^2\right) \log_{\hat{E}}(c_S^\delta)\chi(\delta) \\ &= \sum_{\delta} \left(\log_{\hat{E}}(c_S^\delta) - \frac{a_p}{p}\log_{\hat{E}}(c_S^{\sigma\delta}) + \frac{1}{p}\log_{\hat{E}}(c_S^{\sigma^2\delta})\right) \chi(\delta) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{\delta} \log_{\hat{E}}(c_S^{\delta})\chi(\delta) - \frac{a_p}{p}\sum_{\delta} \log_{\hat{E}}(c_S^{\sigma\delta})\chi(\delta) + \frac{1}{p}\sum_{\delta} \log_{\hat{E}}(c_S^{\sigma^2\delta})\chi(\delta) \\
&= \sum_{\delta} \log_{\hat{E}}(c_S^{\delta})\chi(\delta) - \frac{a_p}{p}\sum_{\delta} \log_{\hat{E}}(c_S^{\delta})\chi(\sigma^{-1}\delta) + \frac{1}{p}\sum_{\delta} \log_{\hat{E}}(c_S^{\delta})\chi(\sigma^{-2}\delta) \\
&\overset{\text{(a)}}{=} \sum_{\delta} \log_{\hat{E}}(c_S^{\delta})\chi(\delta) - \frac{a_p}{p}\chi(p)^{-1}\sum_{\delta} \log_{\hat{E}}(c_S^{\delta})\chi(\delta) + \frac{1}{p}\chi(p)^{-2}\sum_{\delta} \log_{\hat{E}}(c_S^{\delta})\chi(\delta) \\
&= \left(1 - \frac{a_p}{p}\chi(p)^{-1} + \frac{1}{p}\chi(p)^{-2}\right)\sum_{\delta} \log_{\hat{E}}(c_S^{\delta})\chi(\delta), \qquad (5.2.5)
\end{aligned}
$$

where the equality (a) follows from $\chi(\sigma) = \chi(p)$. Combining (5.2.4) and (5.2.5) we complete the proof. □

5.2.2 Relation between Kato's Euler system and Mazur-Tate elements

We first recall the dual exponential map. We put $T = T_p(E)$ and $V = V_p(E)$. For a positive integer S, we have the pairing $(-,-)$ induced by the cup product

$$(-,-) : H^1_f(\mathbb{Q}(S)\otimes\mathbb{Q}_p, V) \times H^1_{/f}(\mathbb{Q}(S)\otimes\mathbb{Q}_p, V) \to \oplus_{\lambda|S}\mathbb{Q}_p \to \mathbb{Q}_p,$$

where the last map is given by $(a_\lambda)_\lambda \mapsto \sum_\lambda a_\lambda$. Then, we have a $\mathbb{Q}_p$-linear map

$$H^1(\mathbb{Q}(S)\otimes\mathbb{Q}_p, V) \to \mathrm{Hom}_{\mathbb{Q}_p}\left(H^1_f(\mathbb{Q}(S)\otimes\mathbb{Q}_p, V), \mathbb{Q}_p\right). \qquad (5.2.6)$$

The exponential map $\exp_{\hat{E}}$ of $\hat{E}$ induces an isomorphism $\mathbb{Q}_p\otimes\mathbb{Q}(S) \to H^1_f(\mathbb{Q}(S)\otimes\mathbb{Q}_p, V)$. By taking the dual, we have a $\mathbb{Q}_p$-linear map

$$\mathrm{Hom}_{\mathbb{Q}_p}\left(H^1_f(\mathbb{Q}(S)\otimes\mathbb{Q}_p, V), \mathbb{Q}_p\right) \to \mathbb{Q}(S)\otimes\mathbb{Q}_p. \qquad (5.2.7)$$

Definition 5.2.5. We denote by $\exp^*_S$ the dual exponential map (associated to ω) defined as the composite of (5.2.6) and (5.2.7)

$$H^1(\mathbb{Q}(S)\otimes\mathbb{Q}_p, V) \to \mathrm{Hom}_{\mathbb{Q}_p}\left(H^1_f(\mathbb{Q}(S)\otimes\mathbb{Q}_p, V), \mathbb{Q}_p\right) \to \mathbb{Q}(S)\otimes\mathbb{Q}_p,$$

We note that for $c \in \hat{E}(\mathscr{O}_S\otimes\mathbb{Z}_p)$ and $z \in H^1(\mathbb{Q}(S)\otimes\mathbb{Q}_p, T)$, we have

$$(c,z) = \mathrm{tr}_{\mathbb{Q}(S)/\mathbb{Q}}\left(\log_{\hat{E}}(c)\cdot\exp^*_S(z)\right) \in \mathbb{Z}_p. \qquad (5.2.8)$$

As in Chapter 4, we denote by $\mathscr{N}$ the set of square-free products of primes relatively prime to pN. Kato constructed the following system (cf. [18, Theorems 9.7 and 12.5]).

Theorem 5.2.6 (Kato [18])**.** *There exists a system* $\{z'_{Sp^n}\}_{S\in\mathscr{N},n\geq 0} \in \prod H^1(\mathbb{Q}(Sp^n), T)$ *such that*

1. *for $S \in \mathscr{N}$, a prime $\ell \nmid pSN$ and $n \geq 0$, we have*

$$\mathrm{Cor}_{S\ell/S}(z'_{S\ell p^n}) = \left(1 - \frac{a_\ell}{\ell}\mathrm{Fr}_\ell^{-1} + \frac{1}{\ell}\mathrm{Fr}_\ell^{-2}\right) z_{Sp^n},$$

2. *for $S \in \mathscr{N}$, the system $\{z'_{Sp^n}\}_{n\geq 0}$ is a norm compatible system,*

3. *for every character χ of Γ_{Sp^n} of conductor Sp^n, we have*

$$\sum_{\gamma\in\Gamma_{Sp^n}} \chi(\gamma)\exp^*_{Sp^n}((z'_{Sp^n})^\gamma) = \left(1 - \frac{a_p\chi(p)}{p} + \frac{\chi^2(p)}{p}\right)\frac{L(E,\chi,1)}{\Omega^+}.$$

We slightly modify this system to construct an Euler system in our sense.

Proposition 5.2.7. *There exists an Euler system $\{\mathfrak{z}_{Sp^n}\}_{S\in\mathscr{N},n\geq 0} \in \prod H^1(\mathbb{Q}(Sp^n), T)$ in the sense of Definition* 4.2.6 *such that for every character χ with conductor Sp^n, we have*

$$\sum_{\gamma\in\Gamma_{Sp^n}} \chi(\gamma)\exp^*_{Sp^n}(\mathfrak{z}^\gamma_{Sp^n}) = \left(1 - \frac{a_p\chi(p)}{p} + \frac{\chi^2(p)}{p}\right)\frac{L(E,\chi,1)}{\Omega^+}.$$

Proof. We put $P_\ell(t) = 1 - a_\ell t + t^2$ as in (4.2.3). Then, since

$$P_\ell(t) \equiv 1 - \frac{a_\ell}{\ell}t + \frac{1}{\ell}t^2 \mod \ell - 1,$$

we apply Proposition 4.2.8 to Kato's Euler system in Theorem 5.2.6, and have our Euler system $\{\mathfrak{z}_{Sp^n}\}$. □

Remark 5.2.8. In [19], [21] and [33], original Kato's Euler system in Theorem 5.2.6 is related to Mazur-Tate elements.

Definition 5.2.9. For a square-free product S of primes relatively prime to pN, we define $\vartheta(\mathfrak{z}_S)$ by

$$\vartheta(\mathfrak{z}_S) = \sum_{\gamma\in\Gamma_S} (c_S, \mathfrak{z}_S^{\gamma^{-1}})\gamma \in \mathbb{Z}_p[\Gamma_S].$$

In order to connect $\vartheta(\mathfrak{z}_S)$ with the Mazur-Tate element θ_S (Definition 3.2.2), we study properties of $\vartheta(\mathfrak{z}_S)$. By abuse of notation, we denote by $\pi_{m/n}$ the natural map $\mathbb{Z}_p[\Gamma_m] \to \mathbb{Z}_p[\Gamma_n]$ for $n|m$.

Proposition 5.2.10. *We have the following:*

1. *Let ℓ be a prime with $\ell \nmid pNS$. Then we have*

$$\pi_{S\ell/S}(\vartheta(\mathfrak{z}_{S\ell})) = -\mathrm{Fr}_\ell(1 - a_\ell\mathrm{Fr}_\ell^{-1} + \mathrm{Fr}_\ell^{-2})\vartheta(\mathfrak{z}_S).$$

2. For every character χ of Γ_S with conductor S, we have

$$\chi(\vartheta(\mathfrak{z}_S)) = \tau_S(\chi)\frac{L(E,\chi^{-1},1)}{\Omega^+}.$$

Proof. By (5.2.8), for $S \in \mathscr{N}$ we have

$$\begin{aligned}\vartheta(\mathfrak{z}_S) &= \sum_{\gamma\in\Gamma_S}(c_S,\mathfrak{z}_S^{\gamma^{-1}})\gamma = \sum_{\gamma\in\Gamma_S}\mathrm{tr}_{\mathbb{Q}(S)/\mathbb{Q}}\left(\log_{\hat{E}}(c_S)\exp_S^*(\mathfrak{z}_S^{\gamma^{-1}})\right)\gamma\\ &= \sum_{\gamma\in\Gamma_S}\sum_{\delta\in\Gamma_S}\log_{\hat{E}}(c_S^\delta)\exp_S^*(\mathfrak{z}_S^{\delta\gamma^{-1}})\gamma = \sum_{\gamma\in\Gamma_S}\sum_{\delta\in\Gamma_S}\log_{\hat{E}}(c_S^\delta)\exp_S^*(\mathfrak{z}_S^{\gamma^{-1}})\delta\gamma\\ &= \left(\sum_{\delta\in\Gamma_S}\log_{\hat{E}}(c_S^\delta)\delta\right)\times\left(\sum_{\gamma\in\Gamma_S}\exp_S^*(\mathfrak{z}_S^{\gamma^{-1}})\gamma\right) \qquad (5.2.9)\end{aligned}$$

in $(\mathbb{Q}(S)\otimes\mathbb{Q}_p)[\Gamma_S]$. By using Proposition 5.2.3, we have

$$\begin{aligned}\pi_{S\ell/S}\left(\sum_{\delta\in\Gamma_{S\ell}}\log_{\hat{E}}(c_{S\ell}^\delta)\delta\right) &= \sum_{\delta\in\Gamma_S}\left(\mathrm{tr}_{\mathbb{Q}(S\ell)/\mathbb{Q}(S)}\left(\log_{\hat{E}}c_{S\ell}\right)\right)^\delta\delta\\ &= -\sum_{\delta\in\Gamma_S}\log_{\hat{E}}\left(c_S^{\mathrm{Fr}_\ell^{-1}\delta}\right)\delta\\ &= -\sum_{\delta\in\Gamma_S}\log_{\hat{E}}\left(c_S^\delta\right)(\delta\mathrm{Fr}_\ell). \qquad (5.2.10)\end{aligned}$$

By Proposition 5.2.7, we have

$$\pi_{S\ell/S}\left(\sum_{\gamma\in\Gamma_{S\ell}}\exp_{S\ell}^*(\mathfrak{z}_{S\ell}^{\gamma^{-1}})\gamma\right) = \sum_{\gamma\in\Gamma_S}\exp_S^*(\mathfrak{z}_S^{\gamma^{-1}})\gamma(1-a_\ell\mathrm{Fr}_\ell^{-1}+\mathrm{Fr}_\ell^{-2}). \qquad (5.2.11)$$

By (5.2.9) (replacing S with $S\ell$), (5.2.10) and (5.2.11), we have

$$\begin{aligned}\pi_{S\ell/S}(\vartheta(\mathfrak{z}_{S\ell})) &= \pi_{S\ell/S}\left(\left(\sum_{\delta\in\Gamma_{S\ell}}\log_{\hat{E}}(c_{S\ell}^\delta)\delta\right)\times\left(\sum_{\gamma\in\Gamma_{S\ell}}\exp_{S\ell}^*(\mathfrak{z}_{S\ell}^{\gamma^{-1}})\gamma\right)\right)\\ &= \left(-\sum_{\delta\in\Gamma_S}\log_{\hat{E}}\left(c_S^\delta\right)(\delta\mathrm{Fr}_\ell)\right)\times\left(\sum_{\gamma\in\Gamma_S}\exp_S^*(\mathfrak{z}_S^{\gamma^{-1}})\gamma(1-a_\ell\mathrm{Fr}_\ell^{-1}+\mathrm{Fr}_\ell^{-2})\right)\\ &= -\mathrm{Fr}_\ell(1-a_\ell\mathrm{Fr}_\ell^{-1}+\mathrm{Fr}_\ell^{-2})\vartheta(\mathfrak{z}_S),\end{aligned}$$

which shows the assertion 1.

By using Propositions 5.2.4 and 5.2.7, we have

$$\chi(\vartheta(\mathfrak{z}_S)) = \left(\sum_{\delta\in\Gamma_S}\log_{\hat{E}}(c_S^\delta)\chi(\delta)\right)\times\left(\sum_{\gamma\in\Gamma_S}\exp_S^*(\mathfrak{z}_S^{\gamma^{-1}})\chi(\gamma)\right)$$

$$= \left(\sum_{\delta \in \Gamma_S} \log_{\hat{E}}(c_S^{\delta}) \chi(\delta) \right) \times \left(1 - \frac{a_p}{p} \chi(p)^{-1} + \frac{1}{p} \chi^{-2}(p) \right) \frac{L(E, \chi^{-1}, 1)}{\Omega^+}$$
$$= \tau_S(\chi) \frac{L(E, \chi^{-1}, 1)}{\Omega^+}.$$

□

We denote by $\theta_{S,p} \in \mathbb{Z}_p[\Gamma_S]$ the image of the Mazur-Tate element θ_S under the natural map $\mathbb{Z}_p[G_S] \to \mathbb{Z}_p[\Gamma_S]$.

Corollary 5.2.11. *For a square-free product S of primes relatively prime to pN, we have*

$$\vartheta(\mathfrak{z}_S) = \theta_{S,p} \in \mathbb{Z}_p[\Gamma_S],$$

Proof. Combining the proposition above with Proposition 3.2.4, we have

$$\chi(\theta_{S,p}) = \chi(\vartheta(\mathfrak{z}_S)) \quad \text{for all the characters } \chi \text{ of } \Gamma_S,$$

which shows that the element $\theta_{S,p} - \vartheta(\mathfrak{z}_S) \in \mathbb{Q}_p[\Gamma_S]$ belongs to all maximal ideals of $\mathbb{Q}_p[\Gamma_S]$. Hence, we have $\theta_S^{(p)} = \vartheta(\mathfrak{z}_S)$. □

For a finite abelian group G, we denote by I_G the augmentation ideal of $\mathbb{Z}_p[G]$. As in Chapter 4, we put

$$\mathfrak{r}_{\min} = \min_{n \geq 1} \{ r_{p^n} \left(H^1_{f,p}(\mathbb{Q}, E[p^n]) \right) \}.$$

Corollary 5.2.12. *Let S be a square-free product of primes ℓ relatively prime to N with the following condition: if $\ell \equiv 1 \mod p$, then $E(\mathbb{F}_\ell)[p]$ is cyclic, that is, $E(\mathbb{F}_\ell)[p]$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or 0. Then, we have*

$$\theta_S \in I_{G_S}^{\min\{\mathfrak{r}_{\min},\ p\}}.$$

Proof. We first assume that $(S, p) = 1$. By Lemma 5.1.2, we are reduced to proving that $\theta_{S,p} \in I_{\Gamma_S}^{\min\{\mathfrak{r}_{\min},\ p\}}$. Since the $\mathbb{Z}_p$-linear map $H^1(\mathbb{Q}(S) \otimes \mathbb{Q}_p, T) \to \mathbb{Z}_p;\ x \mapsto (c_S, x)$ induces $H^1(\mathbb{Q}(S) \otimes \mathbb{Q}_p, T) \otimes_{\mathbb{Z}_p} I_{\Gamma_S}^t \to I_{\Gamma_S}^t$ for all $t \geq 0$, Corollary 4.3.13 implies that $\vartheta(\mathfrak{z}_S) \in I_{\Gamma_S}^{\min\{\mathfrak{r}_{\min},\ p\}}$. Hence, by Corollary 5.2.11, we have

$$\theta_{S,p} \in I_{\Gamma_S}^{\min\{\mathfrak{r}_{\min},\ p\}}.$$

Next, we assume that $(S, p) \neq 1$. If we put $S' = S/p$, then $p \nmid S'$. By the case above and Proposition 3.2.4, we have

$$\pi_{S/S'}(\theta_S) = -\mathrm{Fr}_p(1 - a_p \mathrm{Fr}_p^{-1} + \mathrm{Fr}_p^{-2}) \theta_{S'} \in I_{G_{S'}}^{\min\{\mathfrak{r}_{\min},\ p\}}.$$

Hence, by Lemma 5.1.2 and $p \nmid |G_p|$, we obtain $\theta_S \in I_{G_S}^{\min\{\mathfrak{r}_{\min},\ p\}}$. □

We put $r_{p^\infty} = \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}(\mathbb{Q}, E[p^\infty]))$. Since $\mathrm{Sel}(\mathbb{Q}, E[p^n]) \to \mathrm{Sel}(\mathbb{Q}, E[p^\infty])[p^n]$ is surjective (cf. [36, Lemma 1.5.4]), we have

$$r_{p^n}(\mathrm{Sel}(\mathbb{Q}, E[p^n])) \geq r_{p^n}\left(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])[p^n]\right) \geq r_{p^\infty} \tag{5.2.12}$$

for $n \geq 1$. Since $p \nmid |E(\mathbb{F}_p)|$, we have $E(\mathbb{Q}_p)/p \cong \mathbb{Z}/p\mathbb{Z}$. By Lemma 4.3.3 with the exact sequence

$$0 \to H^1_{f,p}(\mathbb{Q}, E[p^n]) \to \mathrm{Sel}(\mathbb{Q}, E[p^n]) \to E(\mathbb{Q}_p)/p^n,$$

we have

$$r_{p^n}(H^1_{f,p}(\mathbb{Q}, E[p^n])) \geq r_{p^n}(\mathrm{Sel}(\mathbb{Q}, E[p^n])) - 1 \quad \text{for } n \geq 1. \tag{5.2.13}$$

By (5.2.12) and (5.2.13),

$$\mathfrak{r}_{\min} \geq r_{p^\infty} - 1.$$

Hence, by Corollary 5.2.12, we obtain the following:

Corollary 5.2.13. *Let S be a square-free product of primes ℓ relatively prime to N with the following condition: if $\ell \equiv 1 \mod p$, then $E(\mathbb{F}_\ell)[p]$ is cyclic. Then, when $r_{p^\infty} \geq 1$, we have*

$$\theta_S \in I_{G_S}^{\min\{r_{p^\infty}-1, p\}}.$$

5.3 Application of the p-parity conjecture

In this section, we apply the p-parity conjecture, and prove Theorem 5.3.2. We keep the notation and assumption as in Section 5.2.

First, following [28, Chapter 1, §6], we recall the functional equation of Mazur-Tate elements. Let w_N be the operator defined in Definition 3.1.7. We denote by f the newform corresponding to E. Then, there exits $\varepsilon_f \in \{\pm 1\}$ such that

$$w_N(f) = -\varepsilon_f f.$$

It is known that

$$\varepsilon_f = (-1)^{\mathrm{ord}_{s=1}(L(E,s))}. \tag{5.3.1}$$

Let S be a positive integer relatively prime to N. By Proposition 3.1.8 (with $\epsilon(-S) = 1$), for an integer a relatively prime to S, we have

$$[a/S]^{\pm}_E = \varepsilon_f \, [a'/S]^{\pm}_E, \tag{5.3.2}$$

where a' is an integer satisfying $a'aN \equiv -1 \mod S$. Let ι be the map $\mathbb{Q}[G_S] \to \mathbb{Q}[G_S]$ sending $\sigma \in G_S$ to σ^{-1}. We have a functional equation of Mazur-Tate elements as follows.

Proposition 5.3.1.

$$\theta_S = \varepsilon_f \delta_{-N}^{-1} \iota(\theta_S),$$

where $\delta_b \in G_S$ corresponds to $b \in (\mathbb{Z}/S\mathbb{Z})^\times$ under the isomorphism $G_S \cong (\mathbb{Z}/S\mathbb{Z})^\times$.

Proof. We have

$$\begin{aligned}
\varepsilon_f \delta_{-N}^{-1} \iota(\theta_S) &= \varepsilon_f \delta_{-N}^{-1} \sum_{a \in (\mathbb{Z}/S\mathbb{Z})^\times} \left(\left[\frac{a}{S}\right]_E^+ + \left[\frac{a}{S}\right]_E^- \right) \delta_a^{-1} \\
&= \varepsilon_f \sum_{a \in (\mathbb{Z}/S\mathbb{Z})^\times} \left(\left[\frac{a}{S}\right]_E^+ + \left[\frac{a}{S}\right]_E^- \right) \delta_{(-aN)^{-1}} \\
&\overset{\text{(a)}}{=} \sum_{a \in (\mathbb{Z}/S\mathbb{Z})^\times} \left(\left[\frac{a'}{S}\right]_E^+ + \left[\frac{a'}{S}\right]_E^- \right) \delta_{a'} \\
&= \theta_S,
\end{aligned}$$

where the equation (a) follows from (5.3.2). □

For $\gamma \in G_S$, we have

$$\iota(\gamma - 1) = \gamma^{-1} - 1 \equiv -\gamma^{-1}(\gamma - 1) \equiv -(\gamma - 1) \mod I_{G_S}^2.$$

Then, we have $\iota = -1$ on $I_{G_S}/I_{G_S}^2$, and similarly $\iota = (-1)^t$ on $I_{G_S}^t/I_{G_S}^{t+1}$ for $t \geq 1$.

Theorem 5.3.2. *We suppose that p does not divide $6N \cdot |E(\mathbb{F}_p)| \prod_{\ell | N} m_\ell$ and the Galois representation $G_\mathbb{Q} \to \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E))$ is surjective. Let S be a square-free product of primes ℓ relatively prime to N with the following condition: if $\ell \equiv 1 \mod p$ then $E(\mathbb{F}_\ell)[p]$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or 0. Then, we have*

$$\theta_S \in I_{G_S}^{\min\{r_{p^\infty}, p\}} \quad \text{in} \quad \mathbb{Z}_p[G_S].$$

Proof. By Corollary 5.2.13, we have $\theta_S \in I_{G_S}^{\min\{r_{p^\infty}-1, p\}}$. If $p \leq r_{p^\infty} - 1$ or $r_{p^\infty} = 0$, then there is nothing to prove. Hence, we assume that $1 \leq r_{p^\infty} \leq p$, and then $\theta_S \in I_{G_S}^{r_{p^\infty}-1}$. We note that the group G_S acts on $I_{G_S}^{r_{p^\infty}-1}/I_{G_S}^{r_{p^\infty}}$ trivially. Then, in $I_{G_S}^{r_{p^\infty}-1}/I_{G_S}^{r_{p^\infty}}$, we have

$$\theta_S = \varepsilon_f \delta_{-N}^{-1} \iota(\theta_S) = \varepsilon_f \delta_{-N}^{-1} (-1)^{r_{p^\infty}-1} \theta_S = \varepsilon_f (-1)^{r_{p^\infty}-1} \theta_S. \tag{5.3.3}$$

The p-parity conjecture (Theorem 2.2.5) asserts that

$$(-1)^{\mathrm{ord}_{s=1}(L(E,s))} = (-1)^{r_{p^\infty}}.$$

Combining this with (5.3.1), by (5.3.3), we have

$$2\theta_S = 0 \quad \text{in } I_{G_S}^{r_{p^\infty}-1}/I_{G_S}^{r_{p^\infty}}.$$

Since 2 is assumed to be invertible in $\mathbb{Z}_p$, we conclude that $\theta_S \in I_{G_S}^{r_{p^\infty}}$. □

5.4 The order of vanishing and leading coefficients of Mazur-Tate elements

In this section, we prove the main result on the Mazur-Tate refined conjecture. We put $r_E = \mathrm{rank}(E(\mathbb{Q}))$. Let R be a subring of $\mathbb{Q}$ on which the primes satisfying at least one of the following conditions are invertible:

1. p divides $6N \cdot |E(\mathbb{F}_p)| \prod_{\ell|N} m_\ell$,
2. the Galois representation $G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E))$ is *not* surjective,
3. $p < r_E$.

For a square-free product S of good primes, we denote by I_S the augmentation ideal of $R[G_S]$.

Theorem 5.4.1. *Let S be a square-free product of good primes ℓ with the following condition: if $\ell \equiv 1 \mod p$ for a prime p not invertible in R, then $E(\mathbb{F}_\ell)[p]$ is cyclic (cf. (2.1.1)). Then, we have*

$$\theta_S \in I_S^{r_E}.$$

Proof. For each prime p not invertible in R, we see that S satisfies the assumption of Theorem 5.3.2. Then, we have $\theta_S \in \mathbb{Z}_p \otimes_R I_S^{r_E}$. By Lemma 5.1.4, we complete the proof. □

Finally, we prove the result on leading coefficients of Mazur-Tate elements. As in Subsection 3.3.2, for each integer S relatively prime to N, we denote by J_S the order of the cokernel of the natural map

$$E(\mathbb{Q}) \to \left(\oplus_{\ell|S} E(\mathbb{F}_\ell)\right) \oplus \left(\oplus_{\ell|N} E(\mathbb{Q}_\ell)/E_0(\mathbb{Q}_\ell)\right).$$

We take S as in Theorem 5.4.1. Let p be a prime not invertible in R such that $p \nmid S$. As in Chapter 4, we denote by $\mathscr{R}_p$ the set of good primes ℓ such that $\ell \equiv 1 \mod p$. We then write $S = \ell_1 \cdots \ell_s$, where $\ell_1, \ell_2, \ldots, \ell_n \in \mathscr{R}_p$, and $\ell_{n+1}, \ldots, \ell_s \notin \mathscr{R}_p$. We put $S_1 = \ell_1 \cdots \ell_n$ and $S_2 = \ell_{n+1} \cdots \ell_s$. We denote by $\widetilde{\theta}_S^{(p)}$ the image of θ_S in $\mathbb{Z}/p\mathbb{Z} \otimes_R I_S^{r_E}/I_S^{r_E+1}$.

Theorem 5.4.2. *If $\widetilde{\theta}_S^{(p)} \neq 0$, then we have*

$$Ш[p] = 0, \qquad p \nmid J_{S_1}, \qquad p \nmid \prod_{\ell|S_2} (a_\ell - 2).$$

Remark 5.4.3. 1. Since $[G_S : G_S^+] = 2$, by using Lemma 5.1.3, we have the same theorem for the image of $\frac{1}{2}\theta_S$ in $I_{G_S^+}^r/I_{G_S^+}^{r+1}$ as in Conjecture 3.3.7.

2. If $S = S_1$, then this theorem is Theorem 1.3.5.

PROOF. Let $\Gamma_S, \theta_{S,p}, I_{\Gamma_S}$ be as in Section 5.2.

First, we assume that $r_E \geq 1$. We denote by $\widetilde{\theta}_{S,p}^{(p)}$ the image of $\theta_{S,p}$ in $\mathbb{Z}/p\mathbb{Z} \otimes I_{\Gamma_S}^{r_E}/I_{\Gamma_S}^{r_E+1}$. Then by Lemma 5.1.3, we have

$$\widetilde{\theta}_{S,p}^{(p)} \neq 0. \tag{5.4.1}$$

By applying Proposition 4.1.5 to $\sum_{\gamma \in \Gamma_S} \mathfrak{z}_S^{\gamma^{-1}} \otimes \gamma$ and by using Corollary 5.2.11, we have

$$\theta_{S,p} = \sum_{\underline{k}=(k_1,\ldots,k_s) \in \mathbb{Z}_{\geq 0}^{\oplus s}} (c_S, D_{\underline{k}} \mathfrak{z}_S)(\sigma_{\ell_1}^{-1} - 1)^{k_1} \cdots (\sigma_{\ell_s}^{-1} - 1)^{k_s}.$$

By Lemma 5.1.1,

$$\theta_{S,p} \equiv \sum_{\substack{k_1+\cdots+k_n \leq r_E \\ k_{n+1}=\cdots=k_s=0}} (c_S, D_{\underline{k}} \mathfrak{z}_S)(\sigma_{\ell_1}^{-1} - 1)^{k_1} \cdots (\sigma_{\ell_s}^{-1} - 1)^{k_s} \mod I_{\Gamma_S}^{r_E+1}.$$

For $\underline{k}$ such that $k_1 + \cdots + k_n < r_E$ and $k_{n+1} = \cdots = k_s = 0$, we have $D_{\underline{k}} = N_{S_2} D'$, where $D' = D_{\ell_1}^{(k_1)} \cdots D_{\ell_n}^{(k_n)}$. We put $S' = \mathrm{Cond}(D')$. By applying Lemma 4.3.3 to the exact sequence

$$0 \to H^1_{f,S'}(\mathbb{Q}, E[p]) \to \mathrm{Sel}(\mathbb{Q}, E[p]) \to \oplus_{\ell | S'} E(\mathbb{Q}_\ell)/p,$$

we have $r_E \leq r_p(H^1_{f,S'}(\mathbb{Q}, E[p])) + r_p(A(S'))$. By applying Theorem 4.4.2 to $D' \mathfrak{z}_{S_1}$, we have

$$\begin{aligned} \mathrm{loc}_p(D \mathfrak{z}_S) = \mathrm{loc}_p(N_{S_2} D' \mathfrak{z}_S) &= \left(\prod_{\ell | S_2} (1 - a_\ell \mathrm{Fr}_\ell^{-1} + \mathrm{Fr}_\ell^{-2}) \right) \mathrm{loc}_p(D' \mathfrak{z}_{S_1}) \\ &\in H^1_f(\mathbb{Q}(S) \otimes \mathbb{Q}_p, E[p]). \end{aligned}$$

Under the pairing $(-,-)$, the group $H^1_f(\mathbb{Q}(S) \otimes \mathbb{Q}_p, E[p])$ is the orthogonal complement of $H^1_{/f}(\mathbb{Q}(S) \otimes \mathbb{Q}_p, E[p])$. Then, we have $(c_S, D \mathfrak{z}_S) \equiv 0 \mod p$. Hence, we obtain

$$\theta_{S,p} \equiv \sum_{\substack{k_1+\cdots+k_n = r_E \\ k_{n+1}=\cdots=k_s=0}} (c_S, D_{\underline{k}} \mathfrak{z}_S)(\sigma_{\ell_1}^{-1} - 1)^{k_1} \cdots (\sigma_{\ell_s}^{-1} - 1)^{k_s} \mod p\mathbb{Z}_p[\Gamma_S] + I_{\Gamma_S}^{r_E+1}.$$

By (5.4.1), there exists $\underline{k}$ such that $k_1 + \cdots + k_n = r_E$, $k_{n+1} = \cdots = k_s = 0$ and $(c_S, D_{\underline{k}} \mathfrak{z}_S) \not\equiv 0 \mod p$. Hence, for D' as above, we have

$$\mathrm{loc}_p(D' \mathfrak{z}_{S_1}) \notin H^1_f(\mathbb{Q}(S_1) \otimes \mathbb{Q}_p, E[p]).$$

Since $\mathrm{ord}(D') = r_E$, Corollary 4.4.3 implies that $Ш[p] = 0$ and that the natural map $E(\mathbb{Q})/p \to \oplus_{\ell|S_1} E(\mathbb{Q}_\ell)/p$ is surjective. In addition, since $p \nmid \prod_{\ell|N} m_\ell$, the natural map $E(\mathbb{Q}) \to \left[\left(\oplus_{\ell|S_1} E(\mathbb{F}_\ell)\right) \oplus \left(\oplus_{\ell|N} E(\mathbb{Q}_\ell)/E_0(\mathbb{Q}_\ell)\right)\right] \otimes \mathbb{Z}/p\mathbb{Z}$ is surjective, that is, $p \nmid J_{S_1}$.

Since Γ_{S_1} acts on $I_{S_1}^{r_E}/I_{S_1}^{r_E+1}$ trivially and $\theta_{S_1} \in I_S^{r_E}$, we have

$$\begin{aligned}
\pi_{S/S_1}(\theta_S) &\equiv \left(\prod_{\ell|S_2}(1 - a_\ell \mathrm{Fr}_\ell^{-1} + \mathrm{Fr}_\ell^{-2})\right)\theta_{S_1} \\
&\equiv \left(\prod_{\ell|S_2}(1 - a_\ell + 1)\right)\theta_{S_1} \\
&\equiv \left(\prod_{\ell|S_2}(2 - a_\ell)\right)\theta_{S_1} \qquad \bmod I_{S_1}^{r_E+1}. \qquad (5.4.2)
\end{aligned}$$

Since $p \nmid |G_\ell|$ for $\ell|S_2$, by Lemma 5.1.3, the image of $\pi_{S/S_1}(\theta_S)$ in $\mathbb{Z}/p\mathbb{Z} \otimes I_{S_1}^{r_E}/I_{S_1}^{r_E+1}$ is not zero. Hence, by (5.4.2), we obtain $p \nmid \prod_{\ell|S_2}(a_\ell - 2)$.

We assume that $r_E = 0$. If we denote by π the natural map $R[G_S] \to R$ sending every $\sigma \in G_S$ to 1, then by Proposition 3.2.4, we have

$$\pi(\theta_S) = \left(\prod_{\ell|S}(a_\ell - 2)\right)\theta_1 = \left(\prod_{\ell|S}(a_\ell - 2)\right)\frac{L(E,1)}{\Omega^+} \in R. \qquad (5.4.3)$$

Hence, since $\pi(\theta_S) \not\equiv 0 \mod p$, we have $L(E,1) \neq 0$. By the work of Kolyvagin and Kato (cf. [36, Theorem 3.5.11]), we have $Ш[p] = 0$. The equation (5.4.3) also implies that

$$p \nmid \prod_{\ell|S}(a_\ell - 2). \qquad (5.4.4)$$

Since $r_E = 0$ and $E(\mathbb{Q})[p] = 0$, we have $E(\mathbb{Q})/p = 0$. We note that $|E(\mathbb{F}_\ell)| \equiv 2 - a_\ell$ for $\ell \in \mathscr{R}_{E,p}$. Then by (5.4.4), we have $p \nmid \prod_{\ell|S_1} |E(\mathbb{F}_\ell)|$, and hence $p \nmid J_{S_1}$. □

Bibliography

[1] A. A. Beĭlinson, Higher regulators and values of L-functions (Russian), *Current problems in mathematics.* **24**, *Itogi Nauki i Tekhniki*, 181–238, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1984.

[2] M. Bertolini and H. Darmon, Derived heights and generalized Mazur-Tate regulators, *Duke Math. J.* **76** (1994), 75–111.

[3] S. Bloch, Algebraic cycles and values of L-functions, *J. Reine Angew. Math.* **350** (1984), 94–108.

[4] S. Bloch, Height pairings for algebraic cycles, *Proceedings of the Luminy conference on algebraic K-theory* (Luminy, 1983), *J. Pure Appl. Algebra* **34** (1984), 119–145.

[5] S. Bloch and K. Kato, L-functions and Tamagawa numbers of motives, *The Grothendieck Festschrift, Vol. I, Progr. Math.* **86**, 333–400, Birkhäuser Boston, Boston, MA, 1990.

[6] C. Breuil, B. Conrad, F. Diamond and R. Taylor, On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2011), 843–939.

[7] A. C. Cojocaru, On the surjectivity of the Galois representations associated to non-CM elliptic curves, *Canad. Math. Bull.* **48** (2005), 16–31.

[8] H. Darmon, A refined conjecture of Mazur-Tate type for Heegner points, *Invent. Math.* **110** (1992), 123–146.

[9] H. Darmon, Euler systems and refined conjectures of Birch Swinnerton-Dyer type, *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture* (Boston, MA, 1991), *Contemp. Math.* **165**, 265–276, Amer. Math. Soc., Providence, RI, 1994.

[10] H. Darmon, Thaine's method for circular units and a conjecture of Gross, *Canad. J. Math.* **47** (1995), 302–317.

[11] T. Dokchitser, Notes on the parity conjecture, *Elliptic curves, Hilbert modular forms and Galois deformations, Adv. Courses Math. CRM Barcelona*, 201–249, Birkhäuser/Springer, Basel, 2013.

[12] T. Dokchitser and V. Dokchitser, On the Birch-Swinnerton-Dyer quotients modulo squares, *Ann. of Math.* (2) **172** (2010), 567–596.

[13] T. Dokchitser and V. Dokchitser, Root numbers and parity of ranks of elliptic curves, *J. Reine Angew. Math.* **658** (2011), 39–64.

[14] V. G. Drinfel′d, Two theorems on modular curves, *Funkcional. Anal. i Priložen.* **7** (1973), 83–84.

[15] B. H. Gross, On the values of abelian L-functions at $s = 0$, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **35** (1988), 177–197.

[16] R. Gupta and M. R. Murty, Cyclicity and generation of points mod p on elliptic curves, *Invent. Math.* **101** (1990), 225–235.

[17] K. Kato, Euler systems, Iwasawa theory, and Selmer groups, *Kodai Math. J.* **22** (1999), 313–372.

[18] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, *Cohomologies p-adiques et applications, arithmétiques. III, Astérisque* **295** (2004), ix, 117–290.

[19] S. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes, *Invent. Math.* **152** (2003), 1–36.

[20] V. A. Kolyvagin, Euler systems, *The Grothendieck Festschrift, Vol. II, Progr. Math.* **87**, 435–483, Birkhäuser Boston, Boston, MA, 1990.

[21] M. Kurihara, On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I, *Invent. Math.* **149** (2002), 195–224.

[22] M. Kurihara, The structure of Selmer groups for elliptic curves and modular symbols, *Iwasawa theory 2012*, *Contrib. Math. Comput. Sci.* **7**, 317–356, Springer, Heidelberg, 2014.

[23] Q. Liu, *Algebraic geometry and arithmetic curves*, *Oxford Graduate Texts in Mathematics* **6**, Oxford University Press, Oxford, 2002.

[24] M. Longo and S. Vigni, A refined Beilinson-Bloch conjecture for motives of modular forms, preprint.

[25] J. I. Manin, Parabolic points and zeta functions of modular curves, *Izv. Akad. Nauk SSSR Ser. Mat.* **36** (1972), 19–66.

[26] B. Mazur, Rational points of abelian varieties with values in towers of number fields, *Invent. Math.* **18** (1972), 183–266.

[27] B. Mazur and J. Tate, Canonical height pairings via biextensions, *Arithmetic and geometry, Vol. I, Progr. Math.* **35**, 195–237, Birkhäuser Boston, Boston, MA, 1983.

[28] B. Mazur and J. Tate, Refined conjectures of the "Birch and Swinnerton-Dyer type", *Duke Math. J.* **54** (1987), 711–750.

[29] B. Mazur, J. Tate and J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Invent. Math.* **84** (1986), 1–48.

[30] J. S. Milne, *Arithmetic duality theorems*, Second, BookSurge, LLC, Charleston, SC, 2006.

[31] J. Nekovář, On the parity of ranks of Selmer groups. IV, *Compos. Math.* **145** (2009), 1351–1359.

[32] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*, Second edition, *Grundlehren der Mathematischen Wissenschaften* [*Fundamental Principles of Mathematical Sciences*] **323**, Springer-Verlag, Berlin, 2008.

[33] R. Otsuki, Construction of a homomorphism concerning Euler systems for an elliptic curve, *Tokyo J. Math.* **32** (2009), 253–278.

[34] B. Perrin-Riou, Fonctions L p-adiques d'une courbe elliptique et points rationnels, *Ann. Inst. Fourier* (Grenoble) **43** (1993), 945–995.

[35] B. Perrin-Riou, Systèmes d'Euler p-adiques et théorie d'Iwasawa, *Ann. Inst. Fourier* (Grenoble) **48** (1998), 1231–1307.

[36] K. Rubin, *Euler systems, Annals of Mathematics Studies* **147**, Princeton University Press, Princeton, NJ, 2000.

[37] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.

[38] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971.

[39] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves, Graduate Texts in Mathematics* **151**, Springer-Verlag, New York, 1994.

[40] J. H. Silverman, *The arithmetic of elliptic curves*, Second edition, *Graduate Texts in Mathematics* **106**, Springer, Dordrecht, 2009.

[41] W. A. Stein et al., *Sage Mathematics Software* (Version 5.6), The Sage Development Team, 2013, http://www.sagemath.org.

[42] G. Stevens, Stickelberger elements and modular parametrizations of elliptic curves, *Invent. Math.* **98** (1989), 75–106.

[43] K.-S. Tan, Refined theorems of the Birch and Swinnerton-Dyer type, *Ann. Inst. Fourier* (Grenoble) **45** (1995), 317–374.

[44] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.* (2) **141** (1995), 553–572.

[45] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* (2) **141** (1995), 443–551.

[46] W. Zhang, Selmer groups and the indivisibility of Heegner points, *Camb. J. Math.* **2** (2014), 191–253.